А. К. СУШКЕВИЧ

ТЕОРИЯ ЧИСЕЛ

ЭЛЕМЕНТАРНЫЙ КУРС

ИЗДАТЕЛЬСТВО
ХАРЬКОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
ИМЕНИ А. М. ГОРЬКОГО
Харьков 1954

Ответственный редактор —
проф. *М. Н. Марчевский*

ПРЕДИСЛОВИЕ

Основой для настоящего учебника элементарного курса теории чисел послужило 2-е издание моего украинского учебника «Теорія чисел», ДНТВУ, 1936. Первые пять глав остались в основном те же, что были и в украинском издании. В первой главе несколько расширены параграфы о простых числах; в остальных главах исключены параграфы, напечатанные мелким шрифтом, содержание которых выходит за рамки обычного элементарного курса теории чисел. Шестая глава украинского издания («Квадратичные формы») исключена совершенно, ибо она не входит в официальную программу курса теории чисел. Вместо неё даны две новые главы: гл. VI — «Некоторые сведения о квадратичных формах» и гл. VII — «Работы по теории чисел русских и советских математиков».

В основном в настоящий учебник включен тот материал, который имеется в официальной программе по теории чисел для физико-математических и механико-математических факультетов государственных университетов, изд. 1952 г. (автор А. Гельфонд).

Предназначается этот учебник для начинающих изучать теорию чисел студентов физико-математического факультета, математического отделения университета или пединститута,— будущих преподавателей математики в средней школе. Поэтому изложение курса — элементарное, насыщенное многочисленными числовыми примерами, уясняющими теорию. В конце каждой главы, кроме седьмой, даются упражнения, в большей своей части тоже вычислительного характера. Обращено внимание на вещи, обычно не входящие в учебники теории чисел, но необходимые для преподавателей математики средней школы, например, десятичные периодические дроби, признаки делимости; подробно изложена теория цепных (непрерывных) дробей.

Последняя, седьмая глава имеет характер обзора; только об оценке числа простых чисел Чебышева сказано довольно подробно.

В заключение считаю своим приятным долгом выразить благодарность профессору Г. И. Дринфельду, который оказал мне любезность, просмотрев рукопись и сделав ряд ценных замечаний.

Проф. *А. Сушкевич*

Харьков, 1 августа 1953 г.

ГЛАВА I

О ДЕЛИМОСТИ ЧИСЕЛ

§ 1. В дальнейшем под буквами a, b, c, ... x, y, ... α, β, ... мы будем подразумевать только целые числа, которые могут быть положительными или отрицательными, известными или неизвестными, постоянными или переменными. Из элементарной арифметики известно, что сумма, разность и произведение целых чисел — тоже целые числа, тогда как частное двух целых чисел в исключительных только случаях есть целое число. Мы докажем для целых чисел следующую основную теорему:

Теорема 1. Если a и b два любых целых числа и $b \neq 0$, то можно найти такие целые числа q и r, что будет:

$$a = bq + r, \tag{1}$$

при этом $0 \leqq r < |b|$*); r и q определяются однозначно.

Доказательство. Предположим сначала, что $a > b > 0$. Рассмотрим *кратные* чиcлá b, т. е. чи́сла: $1.b = b$, $2.b$, $3.b$, ... вообще $k.b$. В силу известной аксиомы Архимеда, при достаточно большом k будет: $k.b > a$. Следовательно, найдется такое натуральное число q, что окажется: $bq \leqq a$, тогда как $b(q+1) > a$. Обозначим: $a - bq = r$; очевидно, $r \geqq 0$; отсюда: $a = bq + r$, но $b(q+1) = bq + b > a$, т. е. $bq + b > bq + r$; таким образом: $r < b$. Для этого случая теорема доказана.

Если $a = b > 0$, то $q = 1$, $r = 0$; если $b > a > 0$, то $q = 0$, $r = a$. Если $a < 0$, $b > 0$, то найдем: $|a| = bq + r$, а следовательно: $a = b(-q) - r$; при $r = 0$ формула (1) доказана. При $r > 0$ обозначим: $b - r = r_1$; $0 < r_1 < b$; $r = b - r_1$ и получим:

$$a = b(-q) - b + r_1 = b(-q-1) + r_1;$$

это — та же формула (1), ибо $0 < r_1 < b$.

Наконец, при $b < 0$ имеем по доказанному:

$$a = |b|\,q + r; \quad 0 \leqq r < |b|;$$

*) Через $|x|$ мы, как обычно, обозначаем абсолютную величину числа x, т. е. при $x > 0$ $|x| = x$; при $x < 0$ $|x| = -x$; $|0| = 0$.

следовательно:

$$a = b(-q) + r,$$

т. е. получаем опять формулу (1).

Докажем теперь, что q и r определяются однозначно.

Пусть мы нашли двумя способами:

$$a = bq + r = bq_1 + r_1, \text{ где } 0 \leqq r < |b|, \ 0 \leqq r_1 < |b|$$

отсюда:

$$bq - bq_1 = r_1 - r; \ b(q - q_1) = r_1 - r.$$

Здесь правая часть меньше, чем $|b|$ по абсолютной величине, тогда как левая часть делится на b; следовательно, $r_1 - r = 0$, $r_1 = r$, $q_1 = q$ и теорема 1 доказана вполне.

Замечание. Нахождение чисел q и r при данных (положительных) a и b — обычное «деление с остатком» натуральных чисел, которому учит элементарная арифметика. Здесь мы строго доказали существование чисел q и r для произвольных целых чисел a и b; q — *неполное частное*, r — *остаток* от деления a на b.

Деля обе части равенства (1) на b, получим:

$$\frac{a}{b} = q + \frac{r}{b}. \tag{2}$$

Здесь левая часть (при $|a| \geqq b > 0$) — неправильная дробь, тогда как $\frac{r}{b}$ всегда правильная дробь; формула (2) представляет выделение целой части из неправильной дроби; q — целая часть дроби $\frac{a}{b}$; она обозначается:

$$q = \left[\frac{a}{b}\right] = E\left(\frac{a}{b}\right).$$

Замечание. Вообще, если x — любое вещественное число (рациональное или иррациональное, положительное или отрицательное), то его *целой частью* $[x]$ или $E(x)$ называется такое целое число $[x]$, что: $[x] \leqq x < [x] + 1$. При x — целом $[x] = x$.

Подобно же вводится обозначение: $\{x\} = x - [x]$; $\{x\}$ — *дробная часть* числа x; всегда $\{x\} \geqq 0$. Наконец, через (x) обозначают *расстояние числа x до ближайшего к x целого числа*, т. е. абсолютную величину разности между x и ближайшим целым числом к x, т. е. наименьшее из чисел: $\{x\}$ и $1 - \{x\}$.

Интересен случай, когда $r = 0$; тогда формула (1) дает $a = bq$, или $\frac{a}{b} = q$. В этом случае говорят: *a делится* на b (т. е. *делится без остатка*), b — *делитель* или *множитель* числа a; a — *кратное* числа b.

§ 2. Теорема 2. Если a делится на b, а b делится на c, то и a делится на c.

Доказательство. Это вытекает из ассоциативного закона для умножения: имеем: $a = bq$, $b = cq_1$, следовательно:

$$a = (cq_1)\,q = c\,(qq_1).$$

Теорема 2 выражает так называемый «закон транзитивности» для делимости.

Теорема 3. Если $a_1, a_2, \ldots a_k$ делятся на c, а $x_1, x_2, \ldots x_k$ любые (целые) числа, то и $a_1x_1 + a_2x_2 + \ldots + a_kx_k$ делится на c.

Доказательство. Это вытекает из дистрибутивного закона:

$$a_1 = cb_1,\ a_2 = cb_2,\ \ldots\ a_k = cb_k;$$

отсюда:

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = c\,(b_1x_1 + b_2x_2 + \ldots + b_kx_k).$$

Теорема 4. Если a делится на b, то вообще $\pm a$ делится на $\pm b$, в частности $|a|$ делится на $|b|$.

Доказательство. $a = bq = (-b)(-q)$; $-a = b\,(-q) = (-b)\,q$.

Теорема 5. Каждое число делится само на себя.

Доказательство. $a = a \cdot 1$.

Теорема 6. ± 1 — делитель всякого числа; кроме ± 1 нет чисел, имеющих такое свойство.

Доказательство. $a = 1 \cdot a = (-1)(-a)$. Если α — делитель всякого числа, то и 1 делится на α; но 1 делится только на ± 1.

Теорема 7. 0 делится на всякое число; кроме нуля нет чисел с таким свойством.

Доказательство. $0 = a \cdot 0$; если $a \neq 0$, то a не может делиться на $a + 1$.

Теорема 4 позволяет в вопросах делимости ограничиться только положительными числами. В данной главе мы поэтому будем под буквами подразумевать не только целые, но и положительные числа. Говоря, например, о делителях числа, мы будем иметь в виду его положительные делители. Вообще в вопросах делимости числа a и $-a$ играют одну и ту же роль; такие числа (различающиеся знаком или множителем -1) называются *ассоциированными.*

§ 3. Общее наименьшее кратное. Пусть $a_1, a_2, \ldots a_n$ — данные (целые, положительные) числа; их произведение $a_1a_2 \ldots a_n$ делится на каждое из них, т. е. является их общим кратным. Таких общих кратных — бесчисленное множество, ибо $ka_1a_2 \ldots a_n$ при любом целом k — тоже общее кратное данных чисел; число 0 тоже их общее кратное. Следовательно, существует наименьшее *положительное* кратное этих чисел. Это — так называемое *общее наименьшее кратное*; обозначим его через m.

Обозначают: $m = \mathrm{M}(a_1, a_2, \ldots a_n) = \{a_1, a_2, \ldots a_n\}$.

Очевидно, $0 < m \leqq a_1a_2 \ldots a_n$.

Пусть m_1 какое-нибудь иное общее кратное тех же чисел $a_1, a_2, \ldots a_n$; делим m_1 на m и получаем по теореме 1:

$$m_1 = mq + r;\quad 0 \leqq r < m.$$

Отсюда $r = m_1 - mq$, и по теореме 3 мы выводим, что r — тоже общее кратное чисел $a_1, a_2, \ldots a_n$. Но $r < m$, а m — *наименьшее* общее кратное; следовательно, $r = 0$, и мы получаем:

Теорема 8. Среди всех кратных нескольких данных чисел всегда найдется такое, которое является делителем всякого другого общего кратного этих чисел; это — общее наименьшее кратное.

§ 4. Общий наибольший делитель. Любые n (целых положительных) чисел всегда имеют общий делитель, равный 1. Если кроме 1 (лучше сказать,— кроме ± 1) они не имеют общих делителей, то такие числа называются *взаимно-простыми*. Но может случиться, что кроме 1 данные числа имеют другие общие делители (например, если все они четные, то 2 — тоже их общий делитель). Во всяком случае число общих делителей данных чисел конечно, ибо каждый из них (по абсолютной величине) не может быть больше наименьшего из данных чисел. Пусть d', d'', d''', ... все (положительные) общие делители данных чисел и

$$d = M(d', d'', d''', \ldots).$$

Каждое из данных чисел $a_1, a_2, \ldots a_n$ — общее кратное всех делителей d', d'', d''', ..., а следовательно (по теореме 8), делится и на d. Таким образом, d — тоже общий делитель всех данных чисел, т. е. входит в совокупность чисел d', d'', d''', ... При этом d, очевидно, наибольший из всех этих делителей, ибо он делится на каждый из них. Обозначим:

$$d = D(a_1, a_2, \ldots a_n) = (a_1, a_2, \ldots a_n).$$

Итак:

Теорема 9. Между всеми общими делителями данных чисел имеется такой, который делится на всякий другой общий делитель этих чисел: это — *общий наибольший делитель* данных чисел.

Теорема 10. Число d тогда и только тогда общий наибольший делитель чисел $a_1, a_2, \ldots a_n$, когда частные $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ — взаимно-простые.

Доказательство. 1. Пусть $d = D(a_1, a_2, \ldots a_n)$ и пусть частные $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ имеют общий делитель $\delta > 1$. Тогда, следовательно, частные $\frac{a_1}{d\delta}, \frac{a_2}{d\delta}, \ldots \frac{a_n}{d\delta}$ — целые числа, т. е. $a_1, a_2, \ldots a_n$ имеют общий делитель $d\delta > d$, а это противоречит тому, что d — общий *наибольший* делитель.

2. Пусть теперь числа $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ взаимно-простые; пусть d не наибольший общий делитель; тогда по теореме 9 $D(a_1, a_2, \ldots a_n)$ имеет вид: $d\delta$, где $\delta > 1$. Но тогда $\frac{a_1}{d\delta} = \frac{a_1}{d} : \delta$, $\frac{a_2}{d\delta} = \frac{a_2}{d} : \delta$, ... $\frac{a_n}{d\delta} = \frac{a_n}{d} : \delta$ — целые числа, т. е. $\delta > 1$ — общий делитель чисел $\frac{a_1}{d}$,

$\frac{a_2}{d}, \ldots \frac{a_n}{d}$, что́ противоречит тому, что эти числа — взаимно-простые.

Теорема 11. Если $d = D(a_1, a_2, \ldots a_n)$, то $D(a_1k, a_2k, \ldots a_nk) = dk$, $D\left(\frac{a_1}{k}, \frac{a_2}{k}, \ldots \frac{a_n}{k}\right) = \frac{d}{k}$ (последнее — в том случае, если k — один из общих делителей чисел $a_1, a_2, \ldots a_n$).

Доказательство. Это следует из того, что $\frac{a_\lambda}{d} = \frac{a_\lambda k}{dk} = \frac{a_\lambda : k}{d : k}$ на основании теоремы 10.

§ 5. Рассмотрим случай, когда даны два числа a и b. Пусть $m = M(a, b)$; по теореме 8 ab делится на m. Обозначим:

$$\frac{ab}{m} = d;$$

отсюда:

$$\frac{a}{d} = \frac{m}{b}; \quad \frac{b}{d} = \frac{m}{a}.$$

Правые части, а значит, и левые — целые числа, следовательно, d — общий делитель чисел a и b. Пусть d' — какой-нибудь другой их общий делитель, тогда:

$$\frac{ab}{d'} = a \cdot \frac{b}{d'} = b \cdot \frac{a}{d'},$$

т. е. $m' = \frac{ab}{d'}$ — общее кратное чисел a и b. Оно по теореме 8 делится на m:

$$\frac{m'}{m} = \frac{ab}{d'} : \frac{ab}{d} = \frac{d}{d'}.$$

Это — целое число, т. е. d делится на d', значит (см. теорему 9) d — общий *наибольший* делитель чисел a и b.

Итак:

Теорема 12. Если $m = M(a, b)$, $d = D(a, b)$, то

$$ab = md. \tag{3}$$

При $d = 1$ из (3) непосредственно вытекает:

Следствие. Числа a и b взаимно-простые тогда и только тогда, когда их общее наименьшее кратное равно их произведению.

Заметим, что если число данных чисел больше двух, то эта теорема неверна: общее наименьшее кратное взаимно-простых чисел может и не равняться их произведению. Например:

$$D(6, 4, 9) = 1, \text{ тогда как } M(6, 4, 9) = 36 < 6 \cdot 4 \cdot 9.$$

В дальнейшем мы к этому еще вернемся (см. теорему 17).

§ 6. Теорема 13. Чтобы найти общий наибольший делитель нескольких чисел, можно сначала найти общий наибольший делитель каких-нибудь двух из данных чисел, затем найти общий наибольший делитель этого найденного и какого-нибудь третьего из данных чисел, далее найти общий наибольший делитель этого

найденного во второй раз и какого-нибудь четвертого из данных чисел и т. д. Последний из найденных таким образом делителей и есть общий наибольший делитель всех данных чисел.

Доказательство. Достаточно доказать эту теорему для трех данных чисел a, b, c. Аналогично она доказывается и для бо́льшего числа данных чисел. Итак, пусть $D(a, b) = e$, $D(e, c) = d$; по теореме 2 a и b делятся на d, т. е. d — общий делитель для a, b, c. Пусть d' — какой-нибудь другой общий делитель тех же чисел; тогда (по теореме 9) e делится на d', а следовательно (по той же теореме 9), и d делится на d', т. е. d — общий *наибольший* делитель чисел a, b, c. В виде формулы:

$$D(a, b, c) = D(D(a, b), c).$$

Аналогичная теорема существует и для общего наименьшего кратного.

Теорема 14. Чтобы найти общее наименьшее кратное нескольких чисел, можно сначала найти общее наименьшее кратное двух из них, затем найти общее наименьшее кратное этого найденного и третьего из данных чисел и т. д. Последнее из найденных кратных и есть общее наименьшее кратное всех данных чисел.

Эту теорему тоже достаточно доказать только для трех данных чисел a, b, c. Доказательство, вполне аналогичное доказательству теоремы 13 (только вместо теоремы 9 приходится ссылаться на теорему 8), мы предоставляем читателю.

И эту теорему можно выразить формулой:

$$M(a, b, c) = M(M(a, b), c).$$

Таким образом, нахождение общего наибольшего делителя (или общего наименьшего кратного) нескольких чисел сводится к нахождению общего наибольшего делителя (или общего наименьшего кратного) только двух чисел. О практическом способе нахождения общего наибольшего делителя двух чисел мы скажем в следующей главе.

§ 7. Теорема 15. Если ab делится на c, а a и c взаимно-простые, то b делится на c.

Доказательство. ab делится на a и на c, а следовательно (по теореме 8), и на их общее наименьшее кратное, которое по следствию из теоремы 12 равно их произведению: $M(a, c) = ac$; следовательно, $\frac{ab}{ac} = \frac{b}{c}$ — целое число.

Теорема 16. Если a и c — взаимно-простые, то:

$$D(ab, c) = D(b, c).$$

Доказательство. Пусть $D(b, c) = d$; тогда и ab делится на d. Обратно, пусть $D(ab, c) = d$; имеем $D(a, d) = 1$, ибо иначе (по теореме 2) a и c не могли бы быть взаимно-простыми. Следовательно: ab делится на d, но a и d — взаимно-простые; по теореме 15 в таком случае и b делится на d. И теорема доказана.

Заметим, что теорема 15 — частный случай теоремы 16, — при $d = c$.

Если не только $D(a, c) = 1$, но и $D(b, c) = 1$, то теорема 16 дает:

$$D(ab, c) = 1.$$

Значит:

Следствие 1. Если c взаимно-простое с a и с b отдельно, то c взаимно-простое и с произведением ab.

Это следствие непосредственно обобщается и на несколько множителей.

Следствие 2. Если каждое из чисел $a_1, a_2, \ldots a_m$ взаимно-простое с каждым из чисел $b_1, b_2, \ldots b_n$, то и произведения $a_1 a_2 \ldots a_m$ и $b_1 b_2 \ldots b_n$ взаимно-простые.

Если $a_1 = a_2 = \ldots = a_m$ и $b_1 = b_2 = \ldots = b_n$, то получаем:

Следствие 3. Если a и b взаимно-простые, то и всякая степень a взаимно-простая со всякой степенью b *).

§ 8. Исследуем теперь, в каких случаях общее наименьшее кратное нескольких чисел равно их произведению. Пусть даны три числа a, b, c. По теореме 14, чтобы найти $M(a, b, c)$, мы сначала находим $M(a, b)$; если $M(a, b) < ab$, то и $M(a, b, c) < abc$. Следовательно, должно быть $M(a, b) = ab$, а поэтому (по следствию из теоремы 12) $D(a, b) = 1$.

Далее, будем иметь: $M(a, b, c) = M(ab, c)$; чтобы это равнялось abc, должно быть $D(ab, c) = 1$, а отсюда, очевидно, $D(a, c) = 1$, $D(b, c) = 1$. Таким образом, каждая пара чисел a, b, c взаимно-простая, или, как говорят, числа a, b, c «попарно взаимно-простые».

Обратно, пусть теперь дано, что числа a, b, c попарно взаимно-простые; в таком случае $M(a, b) = ab$. По следствию 1 из теоремы 16 ab и c тоже взаимно-простые, значит: $M(a, b, c) = M(ab, c) = abc$.

Это непосредственно обобщается и на несколько чисел.

Итак:

Теорема 17. Общее наименьшее кратное нескольких чисел тогда и только тогда равно их произведению, когда эти числа попарно взаимно-простые.

Следствие. Если число c делится на каждое из чисел $a_1, a_2, \ldots a_n$, а эти числа попарно взаимно-простые, то c делится и на произведение $a_1 a_2 \ldots a_n$.

Это вытекает непосредственно из теорем 17 и 8.

§ 9. Некоторые приложения. 1. Пусть x — целое число; докажем, что если $\sqrt[m]{x}$ не целое число, то этот корень не может быть и рациональной дробью. Предположим, что $\sqrt[m]{x} = \frac{a}{b}$, где $\frac{a}{b}$ — несо-

---

*) При этом, конечно, подразумевается, что показатели всех наших степеней — целые положительные числа.

кратимая дробь, т. е. $D(a, b) = 1$. Тогда $x = \frac{a^m}{b^m}$, и по следствию 3 теоремы 16 дробь $\frac{a^m}{b^m}$ тоже несократима, а следовательно, не может равняться целому числу x при $b > 1$.

Вообще, алгебраическое уравнение n-й степени с целыми коэффициентами и с коэффициентом при высшей степени равным единице не может иметь рациональных дробных корней.

Пусть

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0 \tag{4}$$

такое уравнение и $x = \frac{a}{b}$ его рациональный корень, причем $D(a, b) = 1$. Подставляя это значение x в уравнение (4) и умножая обе части на b^{n-1}, получим:

$$\frac{a^n}{b} + a_1a^{n-1} + a_2ba^{n-2} + \ldots + a_nb^{n-1} = 0.$$

Здесь при $b > 1$ первое слагаемое — дробь (по тому же следствию 3 из теоремы 16), а все остальные — целые числа; такая сумма не может равняться нулю. Следовательно, должно быть $b = 1$, т. е. $x = a$ — целый корень.

Заметим, что корни уравнения типа (4), если они не рациональны, называются *целыми алгебраическими числами*.

2. Рассмотрим *биномиальный коэффициент*:

$$\binom{b}{a} = \frac{b(b-1)(b-2)\ldots(b-a+1)}{1 \cdot 2 \cdot 3 \ldots a}$$

при $b \geqq a$. Имеем:

$$\binom{b}{b} = 1, \quad \binom{b}{1} = b;$$

обозначают еще:

$$\binom{b}{0} = 1, \quad \binom{b}{a} = 0 \text{ при } a > b.$$

Непосредственным вычислением легко вывести формулу:

$$\binom{b}{a} = \binom{b-1}{a} + \binom{b-1}{a-1}. \tag{5}$$

Отсюда методом полной индукции выводим, что $\binom{b}{a}$ всегда целое число. Далее, имеем:

$$\binom{b}{a} = \frac{b}{a}\binom{b-1}{a-1}. \tag{6}$$

Пусть $b > a$ и $D(a, b) = 1$. Из формулы (6) следует, что $b \cdot \binom{b-1}{a-1}$ делится на a, а следовательно, по теореме 15 $\binom{b-1}{a-1}$ делится на a. Но тогда из формулы (6) вытекает, что $\binom{b}{a}$ делится на b.

Таким образом, при взаимно-простых a и b $\binom{b}{a}$ делится на b.

§ 10. Простые числа. Среди всех целых чисел выделяются числа ± 1 и 0; ± 1 имеет только один делитель 1 *); 0 делится на всякое целое число, т. е. имеет бесчисленное множество делителей. Всякое другое целое число a имеет по крайней мере двух делителей: 1 и $|a|$; если оно кроме этих двух делителей не имеет больше ни одного (целого) делителя, то называется *простым*; в противном случае оно *составное*.

Если p — простое число, а a — какое-нибудь другое (целое) число, то общий наибольший делитель чисел a и p равен или p или 1, ибо иных делителей p не имеет. Отсюда получаем:

Теорема 18. Всякое целое число или делится на данное простое число p, или взаимно-простое с p.

А отсюда по теореме 15 следует:

Теорема 19. Произведение (двух или нескольких чисел) делится на простое число p тогда и только тогда, когда по крайней мере один из сомножителей делится на p.

Это весьма важное свойство простых чисел может служить новым их определением. Ибо легко видеть и обратное: если произведение двух чисел делится на p тогда и только тогда, когда один из сомножителей делится на p, то p — простое число.

Действительно, пусть $p = ab$; но p, т. е. ab делится на p, т. е. один из сомножителей, например a, делится на p, т. е. $a = \pm p$, $b = \pm 1$; иных разложений p не может иметь, оно — простое.

Очевидно, что всякое составное число $a (a \neq 0)$ имеет конечное число делителей. Пусть q — наименьший делитель числа a, который > 1; легко видеть, что q — простое число, ибо всякий делитель $k > 1$ числа q был бы делителем и a, а q — наименьший делитель числа a.

Таким образом:

Теорема 20. Всякое целое число кроме единицы имеет по крайней мере один простой делитель.

Итак, пусть a делится на простое число p, $a = pa_1$; a_1 тоже имеет по теореме 20 простой делитель q, $a_1 = qa_2$, откуда: $a = pqa_2$; подобно же и a_2 имеет простой делитель r: $a_2 = ra_3$, $a = pqra_3$; и т. д. Очевидно: $a > a_1 > a_2 > \ldots$ Но множество целых положительных чисел, меньших определенного числа a, конечно. Значит, некоторое a_k будет $= 1$, а a_{k-1} — простое число. Итак, каждое составное число есть произведение конечного числа простых чисел: $a = pqr \ldots$

Докажем, что такое представление числа a возможно только одним способом. Пусть мы нашли два представления:

$$a = pqr \ldots = p_1 q_1 r_1 \ldots ; \qquad (7)$$

---

*) Мы имеем в виду только положительные делители.

здесь: $p, q, r, \ldots p_1, q_1, r_1, \ldots$ — простые числа. Из (7) видно, что $p_1 q_1 r_1 \ldots$ делится на p; следовательно, по теореме 19 один из сомножителей $p_1, q_1, r_1 \ldots$ должен делиться на p. Пусть это будет p_1; но p_1 — простое число, значит, $p_1 = p$, и на p можно сократить обе части (7). Получим:

$$qr \ldots = q_1 r_1 \ldots$$

и аналогично заключим, что q равно одному из чисел $q_1, r_1, \ldots$, например, $q = q_1$; и т. д. Таким образом:

Теорема 21 (основная теорема). Всякое целое число раскладывается, и только одним способом, на простые множители.

Конечно, среди множителей $p, q, r, \ldots$ могут быть и одинаковые; соединив одинаковые множители в степени, получим разложение вида:

$$a = p^{\alpha} q^{\beta} r^{\gamma} \ldots,$$

где $p, q, r, \ldots$ — *различные* простые числа, а $\alpha, \beta, \gamma, \ldots$ — натуральные числа $\geqq 1$.

§ 11. Проблема действительного разложения данного числа на простые множители — одна из труднейших проблем математики; еще не существует практического способа ее разрешения. Приходится просто применять способ испытаний. Специальный случай этой задачи — выяснить, является ли данное число простым. В связи с этим стоит такая задача: найти все простые числа в данном интервале. Еще Эратосфен (в III ст. до нашей эры) предложил следующий способ нахождения всех простых чисел, меньших данного предела A. Выпишем все целые числа, начиная с 2, до числа A; в полученной таблице вычеркнем каждое второе число после 2, каждое третье после 3 (причем надо считать и те числа, которые уже вычеркнуты ранее), каждое пятое число после 5, каждое седьмое число после 7, и т. д. Заметим, что после каждого этапа таких вычеркиваний первое, остающееся незачеркнутым, число обязательно простое, именно, — следующее простое, после которого надо снова начинать вычеркивание. Числа, остающиеся невычеркнутыми в нашей таблице после всех таких вычеркиваний, и будут всеми простыми числами, меньшими, чем A. Ибо ведь мы вычеркнули все составные числа, меньшие, чем A.

Этот метод, называемый «решетом Эратосфена», имеет тот недостаток, что, несмотря на некоторые упрощения, он очень длинный, если число A велико, а потому и весьма непрактичный.

Сделаем еще два замечания об этом методе.

1. Достаточно выписать все нечетные числа, меньшие, чем A, оставив только вначале 2 (единственное четное простое число), и производить указанные выше вычеркивания, т. е. вычеркивать каждое третье число после 3, каждое пятое после 5 и т. д.

2. Дойдя до первого простого числа, которое $\geqq \sqrt{A}$, следует остановиться: все числа, остающиеся невычеркнутыми, — до самого A, будут простыми. Это следует из теоремы:

Теорема 22. Всякое составное число a непременно делится на некоторое число, которое $\leqq \sqrt{a}$.

Доказательство. Если $a = bc$, то из чисел b, c одно $> \sqrt{a}$, а другое $< \sqrt{a}$, за исключением случая, когда a — точный квадрат; тогда может случиться, что $b = c = \sqrt{a}$.

Эта теорема уменьшает число испытаний при определении, является ли данное число простым, или при разложении числа на простые множители.

Пример на решето Эратосфена. Пусть $A = 100$; имеем таблицу:

2,3,5,7,~~9~~,11,13,~~15~~,17,19,~~21~~,23,~~25~~,~~27~~,29,31
~~33~~,~~35~~,37,~~39~~,41,43,~~45~~,47,~~49~~,~~51~~,53,~~55~~,~~57~~,59,61,~~63~~,~~65~~,
67,~~69~~,71,73,~~75~~,~~77~~,79,~~81~~,83,~~85~~,~~87~~,89,~~91~~,~~93~~,~~95~~,97,~~99~~

Здесь $\sqrt{A} = 10$; следовательно, надо вычеркнуть каждое третье число после 3, каждое пятое после 5, каждое седьмое после 7 и на этом остановиться. Все числа, оставшиеся невычеркнутыми, — простые. Мы видим, что их в первой сотне 25.

§ 12. Сколько же всего имеется простых чисел? Еще Эвклид за 300 лет до нашей эры доказал такую теорему:

Теорема 23. Множество простых чисел бесконечно.

Доказательство Эвклида. Возьмем произведение всех простых чисел, начиная от 2 и кончая некоторым простым числом p, и прибавим к этому произведению единицу:

$$P = (2 \cdot 3 \cdot 5 \cdot 7 \ldots p) + 1.$$

Число P не делится ни на 2, ни на 3, ... ни на p, ибо первое слагаемое делится на все эти числа, а второе — не делится (оно $= 1$). Следовательно, P делится на простые числа, бо́льшие, чем p (или само P простое число). Значит, существуют простые числа, большие, чем любое простое число p, т. е. ряд простых чисел беспределен.

З а м е ч а н и е. Вместо того чтобы прибавлять 1 к произведению $2 \cdot 3 \cdot 5 \ldots p$, можно было отнять 1 от этого произведения; можно было распределить все простые числа от 2 до p на два произведения и взять сумму или разность этих произведений:

$$P_1 = (p_1 p_2 \ldots p_k) \pm (q_1 q_2 \ldots q_l);$$

число $|P_1| < P$ или простое, или делится на простые числа $> p$ (за исключением случая, когда $|P_1| = 1$, что может случиться при знаке —).

Доказательство Эйлера. Пусть p_λ — простое число; имеем:

$$\frac{1}{1 - \frac{1}{p_\lambda}} = 1 + \frac{1}{p_\lambda} + \frac{1}{p_\lambda^2} + \ldots = \sum_{k=0}^{\infty} \frac{1}{p_\lambda^k}. \qquad (8)$$

Этот ряд сходящийся, как сумма членов геометрической прогрессии с знаменателем $\frac{1}{p_\lambda} < 1$.

Предположим, что множество простых чисел конечно; пусть

$p_1, p_2, \ldots p_n$ — все простые числа. Напишем ряды (8) при $\lambda = 1, 2, \ldots n$ и перемножим почленно полученные n формул. По известной теореме из теории бесконечных рядов произведение конечного числа сходящихся рядов с положительными членами находят как произведение конечных сумм, умножая каждый член каждого сомножителя на каждый член каждого из остальных сомножителей. Получаемый таким образом ряд — тоже абсолютно-сходящийся, следовательно, его члены можно расположить в любом порядке. Общий член этого ряда имеет вид:

$$\frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}}, \tag{9}$$

где $\alpha_1, \alpha_2, \ldots \alpha_n$ — любые целые показатели ≥ 0. Но по теореме 21 всякое целое положительное число можно представить, при этом однозначно, в виде $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, ибо ведь мы предположили, что существует только n простых чисел $p_1, p_2, \ldots p_n$. Следовательно, (9) имеет вид: $\frac{1}{m}$, где m — любое натуральное число, и произведение рядов (8) можно представить в виде:

$$\sum_{m=1}^{\infty} \frac{1}{m};$$

значит, этот ряд — сходящийся. Но из теории бесконечных рядов известно, что этот так называемый «гармонический» ряд — расходящийся, и мы имеем здесь противоречие. Таким образом, наше предположение о том, что множество простых чисел конечно, — неверно; это множество — бесконечно.

Замечание. Метод, примененный в доказательстве Эйлера, состоит в том, что мы пользуемся понятиями и теоремами из анализа. Это — метод так называемой аналитической теории чисел (простейший пример аналитического метода); эта ветвь теории чисел в своих исследованиях применяет анализ бесконечно малых и с помощью анализа доказывает наиболее глубокие теоремы, относящиеся к числам, в частности, к простым числам.

§ 13. Формула Эйлера. Дадим еще один пример применения аналитических методов к теории чисел, — именно, выведем одну формулу Эйлера, стоящую в связи с приведенным выше его доказательством теоремы о бесчисленном множестве простых чисел.

Если p_λ — любое простое число, а $k > 1$, то имеем:

$$\frac{1}{1 - \frac{1}{p_\lambda^k}} = 1 + \frac{1}{p_\lambda^k} + \frac{1}{p_\lambda^{2k}} + \frac{1}{p_\lambda^{3k}} + \ldots \tag{10}$$

Возьмем все простые числа, не превышающие данного числа N; пусть это будут: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots p_n$. Напишем для них формулы (10) и перемножим эти формулы почленно; так как в правой части (10) — сходящийся ряд с положительными членами, то мы имеем право перемножить эти ряды как обычные

суммы и расположить члены произведения в убывающем порядке. Получим:

$$\prod_{\lambda=1}^{n} \frac{1}{1-\frac{1}{p_\lambda^k}} = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \ldots + \frac{1}{N^k} + \frac{1}{N_1^k} + \frac{1}{N_2^k} + \ldots \quad (11)$$

Так как $p_1, p_2, \ldots p_n$ — все простые числа, меньшие, чем N, то ясно, что в правой части формулы (11) первые N членов будут те, что написаны. Далее $N < N_1 < N_2 < \ldots$, но вообще $N_1 \geqq N + 1$, $N_2 \geqq N_1 + 1$, ..., т. е. уже не все натуральные числа, идущие за N, будут встречаться среди $N_1, N_2, \ldots$

Но при $k > 1$ ряд $1 + \frac{1}{2^k} + \frac{1}{3^k} + \ldots$ — сходящийся, а потому при произвольно-малом $\varepsilon > 0$ можно найти такое натуральное N, что будет:

$$\frac{1}{(N+1)^k} + \frac{1}{(N+2)^k} + \ldots < \varepsilon;$$

а значит, и подавно:

$$\frac{1}{N_1^k} + \frac{1}{N_2^k} + \frac{1}{N_3^k} + \ldots < \varepsilon.$$

Следовательно, при беспредельном возрастании значка n у p_n, т. е. и при беспредельном возрастании N мы получим из формулы (11), что бесконечное произведение $\prod_{\lambda=1}^{\infty} \frac{1}{1-\frac{1}{p_\lambda^k}}$ будет сходящимся и таким образом:

Теорема 24. $$\prod_{\lambda=1}^{\infty} \frac{1}{1-\frac{1}{p_\lambda^k}} = \sum_{m=1}^{\infty} \frac{1}{m^k}. \quad (12)$$

Это и есть формула Эйлера. По существу она выражает, что всякое натуральное число однозначно представляется как произведение простых чисел.

Выведем еще одно важное следствие из формулы (11). Заметим, что она (как и формула (10), из которой (11) выведена) верна и при $k = 1$. Из нее следует:

$$\prod_{\lambda=1}^{n} \frac{1}{1-\frac{1}{p_\lambda}} > \sum_{m=1}^{N} \frac{1}{m}. \quad (13)$$

Пусть теперь N увеличивается беспредельно; тогда и n будет тоже беспредельно возрастать. Но при $N \to \infty$ в правой части (13) мы получим гармонический ряд, который, как известно, расходя-

щийся. Следовательно, и бесконечное произведение $\prod_{\lambda=1}^{\infty} \frac{1}{1-\frac{1}{p_\lambda}}$ расходится, т. е. расходится и ряд $-\sum_{\lambda=1}^{\infty} \ln\left(1-\frac{1}{p_\lambda}\right)$, при этом его сумма $\to +\infty$.

Но $-\ln(1-\eta) = \eta + \frac{\eta^2}{2} + \frac{\eta^3}{3} + \ldots < \eta + \eta^2 + \eta^3 + \ldots = \frac{\eta}{1-\eta} < 2\eta$ при $\eta < 1$. Значит, ряд $2\sum_{\lambda=1}^{\infty} \frac{1}{p_\lambda}$, т. е. и ряд $\sum_{\lambda=1}^{\infty} \frac{1}{p_\lambda}$ расходится.

Итак:

Теорема 25. Ряд: $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots = \sum \frac{1}{p}$, где p пробегает все простые числа,— расходящийся.

§ 14. Мы видели, что в интервале от 1 до 100 (в «первой сотне») имеется 25 простых чисел. Далее, простые числа распределяются следующим образом:

От	До	Простых чисел
101	200	21
201	300	16
301	400	16
401	500	17
501	600	14
601	700	16
701	800	14
801	900	15
901	1000	14

Всего в	первой	тысяче	(от 1	до	1000)	168	простых	чисел
во	второй	»	(» 1001	»	2000)	135	»	»
в	третьей	»	(» 2001	»	3000)	127	»	»
»	четвертой	»	(» 3001	»	4000)	120	»	»
»	пятой	»	(» 4001	»	5000)	119	»	»
»	шестой	»	(» 5001	»	6000)	114	»	»
»	седьмой	»	(» 6001	»	7000)	117	»	»
»	восьмой	»	(» 7001	»	8000)	107	»	»
»	девятой	»	(» 8001	»	9000)	110	»	»
»	десятой	»	(» 9001	»	10000)	112	»	»

Всего от 1 до 10000 . . . . 1229 простых чисел.

Из этих таблиц видно, что простые числа распределены по отдельным сотням и тысячам весьма неправильно, но вообще, если итти от предыдущих до последующих сотен или тысяч, то количество простых чисел постепенно уменьшается. Вопрос о распределении простых чисел в ряде натуральных чисел—один из сложней-

ших вопросов в теории чисел. Знаменитый русский математик П. Л. Чебышев доказал, что количество простых чисел, меньших, чем x, приближенно дается функцией:

$$\int_2^x \frac{dx}{\ln x}.$$

(Подробно об этом см. гл. VII). Этот интеграл представляет собой особую трансцендентную функцию,— так называемый «интегральный логарифм»,— которую нельзя выразить через элементарные функции (алгебраические, тригонометрические, показательную и логарифм).

Интересна задача: найти пределы, между которыми находится по крайней мере одно простое число. В 1845 г. Бертран (Bertrand) высказал предположение, что при $2a > 7$ между a и $2a-2$ лежит по крайней мере одно простое число. Это предположение доказал П. Л. Чебышев в 1852 г. Высказывались и другие предположения; так, Дебов (Desboves) предположил, что между n^2 и $(n+1)^2$ лежит не меньше двух простых чисел.

Гаусс обнаружил, что 26379-я сотня не содержит ни одного простого числа, тогда как 27050-я сотня содержит 17 простых чисел, т. е. больше, чем 3-я сотня. Вообще, можно найти как угодно большие интервалы, совсем не содержащие простых чисел. Так, если p — любое простое число и $P = 2 \cdot 3 \cdot 5 \cdot 7 \ldots p$ — произведение всех простых чисел, кончая числом p, то $P+2$, $P+3$, $P+4$, $\ldots$ $P+p$ — все составные числа.

Единственный случай двух соседних простых чисел — это числа 2 и 3, ибо из двух соседних чисел одно — четное. Но числа вида p, $p+2$ (т. е. соседние нечетные числа) могут быть оба простыми, например, 11, 13; 17, 19; 29, 31; 41, 43; 59, 61; 71, 73; 101, 103; 107, 109. Такие пары называются «простые числа-близнецы». Найдены такие пары и весьма больших чисел, например: 109619, 109621; 10009871, 10009873; 1000061087, 1000061089. Есть основания предполагать, что таких пар «близнецов» бесчисленное множество, но это до сих пор не удалось доказать.

В 1919 г. Брун (Brun) доказал интересную теорему: если простых чисел-«близнецов» и бесчисленное множество, то бесконечный ряд $\sum\left(\frac{1}{p}+\frac{1}{p+2}\right)$, взятый для всех пар p, $p+2$ простых чисел-близнецов,— сходящийся. (Напоминаем, что бесконечный ряд $\sum\frac{1}{p}$, взятый по всем простым числам,— расходящийся, как доказано в теореме 25).

Интересно обобщение теоремы Бруна, которое дал советский математик Б. И. Сегал в 1930 году. Возьмем пары всех простых чисел p, $p+2m$, отличающихся друг от друга на определенное четное (вообще — произвольное) число $2m$; ряд $\sum\left(\frac{1}{p}+\frac{1}{p+2m}\right)$,

взятый по всем таким парам (конечный он или бесконечный), — сходящийся.

Упомянем еще о так называемой проблеме Гольдбаха. Христиан Гольдбах (1690—1764) — математик, работавший в Петербургской Академии наук в 1725—1742 гг. 7 июня 1742 г. в письме к Эйлеру он заметил: «повидимому, всякое число, большее, чем 1, есть сумма трех простых чисел». 30 июня 1742 г. Эйлер ему ответил: «что всякое четное число есть сумма двух простых чисел, я считаю вполне верной теоремой, хотя я и не могу ее доказать».

Эта знаменитая проблема Гольдбаха, над решением которой безуспешно бились многие специалисты по теории чисел, была решена в 1937 г. выдающимся советским математиком Иваном Матвеевичем Виноградовым. Он именно доказал, что всякое нечетное, достаточно большое число представляется как сумма трех простых чисел.

§ 15. Иная проблема, относящаяся к простым числам,— найти функцию от переменного x, которая при всех натуральных значениях x давала бы простые числа (хотя бы не все). Еще Эйлер подбирал такую целую рациональную функцию; его пример: $f(x) = x^2 + x + 41$. Эта функция при $x = 0, 1, 2, \ldots 39$ дает простые числа, но при $x = 40$: $f(40) = 1681 = 41^2$. Найдены еще функции: $x^2 + x + 17$ (имеет простые значения при $x = 0, 1, 2 \ldots 15$); $2x^2 + 29$ (имеет простые значения при $x = 0, 1, 2, \ldots 28$). Но имеется такая теорема:

Теорема 26. Никакая целая рациональная функция от x с целыми коэффициентами не может для всякого натурального значения x равняться простому числу*).

Доказательство. Пусть при $x = a$ (натуральное число) $f(x) = f(a) = \pm p$ (p — простое). При любом целом z $f(a + zp)$ делится на p, ибо если

$$f(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m,$$

то
$$f(a + zp) - f(a) = a_0[(a + zp)^m - a^m] + a_1[(a + zp)^{m-1} - a^{m-1}] + \ldots + a_{m-1}zp;$$

каждый член правой части делится на p и $f(a)$ делится на p. Следовательно, $f(a + zp) = \pm p$, и $f(a + zp)^2 - f(a)^2 = 0$ для бесчисленного множества значений z, т. е. и тождественно: $f(x) = f(a)$ (ибо $x = a + zp$ при любом z может равняться любому числу).

Ферма (Fermat, 1601—1665) высказал предположение, что все числа вида $2^{2^n} + 1$ (при натуральном n) простые. Но это оказалось неверным: при $n = 0, 1, 2, 3, 4$ эти числа действительно простые; но при $n = 5$: $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$, как доказал Эйлер в 1732 г.

---

*) Здесь, конечно, исключается случай, когда функция $f(x) = p = \text{const}$,— постоянно равна простому числу.

При $n = 12$: $2^{2^{12}} + 1$ делится на $7 \cdot 2^{14} + 1 = 114689$; при $n = 23$: $2^{2^{23}} + 1$ делится на $5 \cdot 2^{25} + 1 = 167772161$. Эти случаи разобрал Иван Михеевич Первушин в 1878 г. Число $2^{2^{23}} + 1$ содержит 2525223 цифры. Для напечатания этого числа обыкновенным шрифтом понадобилась бы строка длиною в 5 *км* или книга обыкновенного формата в 1000 страниц.

Зельхоф (Seelhof) в 1886 г. показал, что при $n = 36$ число $2^{2^{36}} + 1$ не простое: оно делится на $5 \cdot 2^{39} + 1 = 2748779069441$. Люка (Lucas) вычислил, что это число $2^{2^{36}} + 1$ содержит более 20 миллиардов цифр; строка с этим числом длинее экватора.

Число $2^{61} - 1 = 2305843009213693951$ — простое, как доказал И. М. Первушин в 1883 г.; оно долгое время считалось самым большим из известных простых чисел. В настоящее время известно, что и числа $2^{89} - 1$ и $2^{107} - 1$ простые. Самое большое из известных в настоящее время простых чисел:

$$2^{127} - 1 = 170141183460469231731687303715884105727.$$

Упомянем еще об одной важной теореме, относящейся к простым числам: если a и b целые взаимно-простые числа, а переменная x пробегает целые значения, то форма $ax + b$ бесчисленное множество раз будет равняться простому числу. Эту теорему доказал Лежен-Дирикле (Lejeune-Dirichlet) в 1837 г. методом аналитической теории чисел. Выражение $ax + b$ есть общий член арифметической прогрессии с первым членом b и с разностью a. Теорема Дирикле, таким образом, показывает, что среди членов арифметической прогрессии, у которой первый член и разность — взаимно-простые числа, имеется бесчисленное множество простых чисел.

Частные случаи этой теоремы: при $a = 4$ существует бесчисленное множество простых чисел вида $4n + 1$ и бесчисленное множество простых чисел вида $4n + 3$ (вместо $4n + 3$ можно взять $4n - 1$); при $a = 3$ существует бесчисленное множество простых чисел вида $3n + 1$ и бесчисленное множество простых чисел вида $3n + 2$ (или $3n - 1$). Заметим, что так как простые числа (кроме 2) нечетны, то в формах $3n \pm 1$ n должно быть четным и вместо $3n + 1$ можно взять форму $6n + 1$, а вместо $3n - 1$ форму $6n - 1$ (или $6n + 5$).

§ 16. Пусть $m = p^{\alpha} q^{\beta} r^{\gamma} \ldots$ — разложение положительного числа m на простые множители; пусть d — делитель числа m. Тогда, очевидно (см. теоремы 2, 19), d не может иметь иных простых множителей, кроме тех, которые входят в m, и каждый из них не может входить в d с показателем, большим, чем тот, с которым он входит в m. Следовательно, d имеет вид:

$$d = p^{\varkappa} q^{\lambda} r^{\mu} \ldots, \qquad (14)$$

где $0 \leqq \varkappa \leqq \alpha$, $0 \leqq \lambda \leqq \beta$, $0 \leqq \mu \leqq \gamma$, ...

Обратно, всякое число вида (14), очевидно, делитель m.

Итак:

Теорема 27. Число m вида $m = p^\alpha q^\beta r^\gamma \ldots$ делится на d тогда и только тогда, когда d имеет вид (14) (с указанными там условиями для $\varkappa$, λ, μ, ...).

Отсюда легко найти число всех делителей данного числа m (включая и 1 и само число m); именно, в (14) $\varkappa$ может принимать $\alpha + 1$ значений, λ может иметь $\beta + 1$ значений, μ - $\gamma + 1$ значений, и т. д. При этом разные комбинации значений $\varkappa$, λ, μ, ... дают и разные числа d. Всего у нас $(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$ разных комбинаций.

Следовательно:

Теорема 28. Число всех возможных делителей данного числа $m = p^\alpha q^\beta r^\gamma \ldots$ есть: $\tau(m) = (\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$

$\tau(m)$ — функция от m, определенная только для целых положительных значений m; такие функции называются арифметическими. Заметим, что $\tau(m)$ зависит только от показателей α, β, γ ..., а не от самих простых множителей p, q, r, ...

Если $d = p^\varkappa q^\lambda r^\mu \ldots$, то $\frac{m}{d} = p^{\alpha-\varkappa} q^{\beta-\lambda} r^{\gamma-\mu} \ldots$; это — так называемый *дополнительный* к d делитель числа m.

Если $m = d^k$, то очевидно: $\alpha = \varkappa k$, $\beta = \lambda k$, $\gamma = \mu k$, ... и обратно.

Таким образом:

Теорема 29. Число $m = p^\alpha q^\beta r^\gamma \ldots$ тогда и только тогда точная k-я степень целого числа, когда α, β, γ, ... все делятся на k.

В частности:

Следствие. Число m тогда и только тогда точный квадрат, когда показатели α, β, γ, ... все четные.

§ 17. Найдем теперь сумму всех делителей данного числа m. Для этого рассмотрим произведение

$$(1 + p + p^2 + \ldots + p^\alpha)(1 + q + q^2 + \ldots + q^\beta)(1 + r + r^2 + \ldots + r^\gamma) \ldots . \qquad (15)$$

Каждый из его сомножителей — сумма членов геометрической прогрессии. Применяя известную из элементарной алгебры формулу для этой суммы, найдем, что произведение (15) равно:

$$\frac{p^{\alpha+1} - 1}{p - 1} \cdot \frac{q^{\beta+1} - 1}{q - 1} \cdot \frac{r^{\gamma+1} - 1}{r - 1} \ldots$$

С другой стороны, применяя известное правило перемножения многочленов, найдем, что (15) имеет вид:

$$\sum_{\varkappa, \lambda, \mu, \ldots} p^\varkappa q^\lambda r^\mu \ldots ,$$

где $\varkappa = 0, 1, 2, \ldots \alpha$; $\lambda = 0, 1, 2, \ldots \beta$; $\mu = 0, 1, 2, \ldots \gamma$; .... т. е. (15) равно сумме $\sum_d d$ всех делителей числа m.

Следовательно:

Теорема 30. Сумма всех делителей числа $m = p^{\alpha}q^{\beta}r^{\gamma} \ldots$ есть:

$$S(m) = \frac{p^{\alpha+1}-1}{p-1} \cdot \frac{q^{\beta+1}-1}{q-1} \cdot \frac{r^{\gamma+1}-1}{r-1} \ldots {}^{*)}$$

Пример: $m = 60 = 2^2 \cdot 3 \cdot 5$; здесь:

$$\tau(60) = 3 \cdot 2 \cdot 2 = 12; \; S\,(60) = \frac{2^3-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 4 \cdot 6 = 168.$$

Действительно, делители числа 60 следующие:

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

Их сумма равна 168.

Само число m есть тоже один из делителей самого себя. Все остальные делители числа m называются *истинными* делителями числа m; их сумма есть $S(m) - m$.

Если для двух чисел a, b сумма истинных делителей каждого из них равняется другому, то такие числа называются *дружественными*; для них $S(a) - a = b$, $S(b) - b = a$, т. е. $S(a) = S(b) = a + b$.

Число, равное сумме своих истинных делителей, называется *совершенным*; для такого числа $S(m) - m = m$, или $S(m) = 2m$.

Понятия о дружественных и совершенных числах были введены еще в Пифагорейской школе древней Греции (в VI в. до нашей эры). Пифагорейцам была известна пара дружественных чисел: 220, 284; были им известны три совершенных числа: 6, 28, 496. Позднее древне-греческие математики нашли еще совершенное число: 8128. Дальнейшие совершенные числа, найденные уже в новое время: 33550336; 8589869056. До сих пор не найдено ни одного нечетного совершенного числа, но и не доказано, что они не существуют.

Л. Эйлер (1707—1783) нашел 65 пар дружественных чисел. Вот одна из найденных им пар: $18416 = 2^4 \cdot 1151$ и $17296 = 2^4 \cdot 23 \cdot 47$.

§ 18. Рассмотрим теперь такую задачу: найти высшую степень простого числа p, на которую делится число $m! = 1 \cdot 2 \ldots m$. Для этого сначала докажем лемму:

Лемма. Чтобы найти неполное частное от деления m на ab, можно сначала m разделить на a и неполное частное от этого деления разделить на b; неполное частное этого второго деления и будет неполным частным от деления m на ab. В виде формулы лемма выразится так:

$$\left[\frac{m}{ab}\right] = \left[\frac{\left[\frac{m}{a}\right]}{b}\right]. \; {}^{**)}$$

---

*) Эту функцию обозначают также знаком $\int(m)$ и называют числовым интегралом от m, взятым по делителям. Такое обозначение ввел Эйлер.

**) Напоминаем, что все наши числа мы считаем не только целыми, но и положительными.

Доказательство. Пусть $m = aq + r$; $q = \left[\frac{m}{a}\right]$, $0 \leqq r < a$, т. е. $0 \leqq r \leqq a - 1$. Пусть, далее, $q = bq_1 + r_1$; $q_1 = \left[\frac{q}{b}\right]$, $0 \leqq r_1 \leqq b - 1$. Подставляя выражение для q в формулу для m, получим:

$$m = a(bq_1 + r_1) + r = (ab)q_1 + (ar_1 + r).$$

Здесь: $0 \leqq ar_1 + r \leqq a(b-1) + a - 1 = ab - 1$, т. е. $0 \leqq ar_1 + r < ab$, а это значит, что $ar_1 + r$ — остаток, q_1 — неполное частное от деления m на ab (см. теорему 1). Так как $q_1 = \left[\frac{\left[\frac{m}{a}\right]}{b}\right]$, то наша лемма доказана.

Замечание. Доказанная лемма верна и при $a = b$.

Пусть теперь p — данное простое число; при $p > m$ очевидно, что $m!$ не делится на p. При $p < m$ в $m!$ входят множители: p, $2p$, $3p$, ... $\left[\frac{m}{p}\right]p$. Кроме них, в $m!$ нет множителей, делящихся на p; эти же дают произведение:

$$p \cdot 2p \cdot 3p \ldots \left[\frac{m}{p}\right]p = \left[\frac{m}{p}\right]!\, p^{\left[\frac{m}{p}\right]}.$$

Таким образом $m!$ делится на $p^{\left[\frac{m}{p}\right]}$ и, кроме того, на ту степень числа p, которая входит в $\left[\frac{m}{p}\right]!$ Но, применяя здесь те же рассуждения, найдем, что множители в $\left[\frac{m}{p}\right]!$, делящиеся на p, дают произведение:

$$p \cdot 2p \cdot 3p \ldots \left[\frac{\left[\frac{m}{p}\right]}{p}\right]p = \left[\frac{m}{p^2}\right]!\, p^{\left[\frac{m}{p^2}\right]},$$

ибо по предыдущей лемме мы имеем:

$$\left[\frac{\left[\frac{m}{p}\right]}{p}\right] = \left[\frac{m}{p^2}\right].$$

Теперь применим те же рассуждения к $\left[\frac{m}{p^2}\right]!$; его множители, делящиеся на p, дают произведение:

$$p \cdot 2p \cdot 3p \ldots \left[\frac{\frac{m}{p^2}}{p}\right]p = \left[\frac{m}{p^3}\right]!\, p^{\left[\frac{m}{p^3}\right]},$$

ибо

$$\left[\frac{\left[\frac{m}{p^2}\right]}{p}\right] = \left[\frac{m}{p^3}\right].$$

И т. д., пока не дойдем до такого показателя λ, что $p^\lambda > m$. Итак:

Теорема 31. Наибольший показатель, с каким простое число p входит множителем в $m!$, есть:

$$\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\left[\frac{m}{p^3}\right]+\ldots+\left[\frac{m}{p^k}\right],$$

где $p^k \leqq m$, но $p^{k+1} > m$. Если уже $p > m$, то $m!$ совсем не делится на p.

Пример. Найти наивысшую степень числа 2, на которую делится 50!

Имеем: $\frac{50}{2}+\left[\frac{50}{4}\right]+\left[\frac{50}{8}\right]+\left[\frac{50}{16}\right]+\left[\frac{50}{32}\right]=47.$

(Мы пишем просто $\frac{50}{2}$, а не $\left[\frac{50}{2}\right]$, ибо $\frac{50}{2}$ — целое число).

Следовательно, 50! делится на 2^{47}.

Замечание. Так можно разложить $m!$ на простые множители, беря за p последовательно все простые числа $< m$.

УПРАЖНЕНИЯ

1. Доказать, что m тогда и только тогда общее наименьшее кратное чисел $a_1, a_2, \ldots a_n$, когда частные $\frac{m}{a_1}, \frac{m}{a_2}, \ldots \frac{m}{a_n}$ взаимно-простые.

(Указание. Доказательство от противного; применить теорему 8, § 3).

2. Доказать, что $M(a_1k,\ a_2k_1,\ \ldots a_nk) = kM(a_1, a_2,\ \ldots a_n)$;

$$M\left(\frac{a_1}{k},\ \frac{a_2}{k},\ \ldots\ \frac{a_n}{k}\right)=\frac{1}{k}M(a_1,\ a_2,\ \ldots\ a_n).$$

Последнее — при условии, что k — общий делитель чисел $a_1, a_2, \ldots a_k$. (Доказательство аналогично доказательству теоремы 11, § 4).

3. Проверить, что $\binom{12}{7}$ делится на 12, $\binom{8}{5}$ делится на 8, $\binom{14}{9}$ делится на 14 (§ 7).

4. Испытаниями (имея в виду теорему 22) выяснить, какие из чисел 437, 509, 811, 1849, 953, 1079, 10519, 17357, 2027 простые, какие составные; последние разложить на простые множители (§ 10).

Ответ. Простые числа: 509, 811, 953, 2027.

5. Применить решето Эратосфена в интервале от 2 до 500 (§ 11).

6. Найти числа $P=(2\cdot 3\cdot 5\ldots p)\pm 1$ при $p=5,\ 7,\ 11,\ 13$; выяснить, какие из них простые, какие составные; последние разложить на простые множители (§ 12).

Ответ. Составные: $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$; $2 \cdot 3 \cdot 5 \times \times 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$; остальные — простые.

7. Найти все простые числа-близнецы < 500 (§ 14).

Ответ. Начиная с числа 11, их 22 пары.

8. Опытным путем найти все представления чисел 64, 100, 466 в виде сумм двух простых чисел (§ 14).

Ответ. Для 64 имеется 5 таких представлений; для 100 их 6; для 466 их 12.

9. Выяснить, сколько простых чисел до 500 имеют форму $4n + 1$, сколько вида $4n + 3$, сколько вида $3n + 1$, сколько вида $3n + 2$ (§ 15).

Ответ. 44 числа вида $4n + 1$;
50 чисел » $4n + 3$;
45 » » $3n + 1$;
50 » » $3n + 2$.

10. Вычислить $\tau(m)$ для $m = 1, 2, 3, \ldots 20$ (§ 16).

11. Найти $\tau(96)$, $\tau(168)$, $\tau(255)$ (§ 16).

Ответ. 12, 16, 8.

12. Доказать, что $\tau(m)$ — всегда четное число, за исключением случаев, когда m — точный квадрат (§ 16).

13. Вычислить $S(m)$ для $m = 1, 2, 3, \ldots 20$ (§ 17).

14. Найти $S(25)$, $S(48)$, $S(72)$, $S(100)$ (§ 17).

Ответ. 31, 124, 195, 217.

15. Обозначив через $S_k(m)$ сумму k-х степеней всех делителей числа $m = p^\alpha q^\beta r^\gamma \ldots$, вывести формулу:

$$S_k(m) = \frac{p^{(\alpha+1)k} - 1}{p^k - 1} \cdot \frac{q^{(\beta+1)k} - 1}{q^k - 1} \cdot \frac{r^{(\gamma+1)k} - 1}{r^k - 1} \ldots \quad (\S\ 17)$$

Указание. Рассмотреть произведение:

$$(1 + p^k + p^{2k} + \ldots + p^{\alpha k})(1 + q^k + q^{2k} + \ldots + q^{\beta k})(1 + r^k + + r^{2k} + \ldots + r^{\gamma k}) \ldots$$

16. Найти $S_2(12)$, $S_2(16)$, $S_3(8)$ (§ 17).

Ответ. 210, 341, 585.

17. Доказать теорему: чтобы найти общий наибольший делитель нескольких чисел, разложенных на простые множители, нужно выписать общие всем данным числам простые множители, каждый с наименьшим показателем, с каким он имеется в разложениях данных чисел.

Произведение этих степеней простых множителей и есть общий наибольший делитель данных чисел.

(Указание. Принять во внимание теорему 27 § 16).

18. Доказать теорему: чтобы найти общее наименьшее кратное нескольких разложенных на простые множители чисел, надо выписать каждый простой множитель, который входит в разложение

хоть одного из данных чисел, с наибольшим показателем, с каким он имеется в разложениях данных чисел.

Произведение всех этих степеней простых чисел и есть общее наименьшее кратное этих чисел.

19. Разложением на простые множители найти: $D(2737, 9163, 9639)$ и $M(2737, 9163, 9369)$. (См. упражнения 17 и 18).

Ответ. 119, 17070669.

20. Разложить на простые множители 100! (§ 18).

21. Найти высшие степени чисел 3, 7, 11, 23, на которые делится число 250! (§ 18).

Ответ. 3^{123}; 7^{40}; 11^{24}; 23^{10}.

ГЛАВА II

АЛГОРИФМ ЭВКЛИДА И ЦЕПНЫЕ ДРОБИ

§ 19. Для практического нахождения общего наибольшего делителя двух чисел существует способ, независимый от разложения данных чисел на простые множители,— это способ последовательного деления или алгорифм Эвклида *). Пусть r и r_1 данные (целые, положительные) числа и $r > r_1$. Делим r на r_1 и обозначаем частное через q_1, остаток через r_2; делим, далее, r_1 на r_2 и обозначаем частное через q_2, остаток через r_3; далее, делим r_2 на r_3, и т. д. Мы имеем: $r_1 > r_2 > r_3 > \ldots \geqq 0$. Следовательно, в конце концов, после n-го деления мы получим остаток, равный нулю: $r_{n+1} = 0$. Таким образом, мы получим равенства (см. (1) в § 1):

$$\left.\begin{aligned} r &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\ldots\ldots\ldots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n \end{aligned}\right\} \qquad (16)$$

Из первого равенства (16) видно, что всякий общий делитель чисел r и r_1 является делителем и числа r_2 (см. § 2, теорема 3); из второго равенства (16) видно, что этот делитель является делителем и числа r_3, и т. д.; наконец, из предпоследнего равенства (16) мы найдем, что этот общий делитель чисел r и r_1 (следовательно, и чисел r_2, r_3, ...) является делителем и числа r_n.

С другой стороны, последнее равенство (16) показывает, что r_{n-1} делится на r_n; предпоследнее (по теореме 3, § 2),— что r_{n-2} делится на r_n, и т. д.; наконец, из второго и первого равенства (16) мы найдем, что r и r_1 делятся на r_n. Следовательно, r_n —

*) Словом «алгорифм» в математике обозначают способ вычислений, состоящий из отдельных звеньев, где каждое следующее звено вычисляется по тем же правилам, как и предыдущее. Это слово — искаженное прозвание узбекского математика первой половины IX века н. э.: Мухаммед ибн Муза аль-Ховаризми (т. е. из Хорезма).

общий делитель чисел r и r_1, который делится на всякий другой общий делитель этих чисел. Такой делитель и есть общий наибольший делитель чисел r и r_1 (см. § 4, теоремы 9). Следовательно:

Теорема 32. Чтобы найти общий наибольший делитель двух чисел, надо большее из данных чисел делить на меньшее; если будет остаток, то следует, далее, меньшее делить на этот остаток; далее, этот первый остаток делить на второй остаток (от второго деления); второй остаток делить на третий остаток и т. д., пока не дойдем до деления, где остаток будет равен нулю. Делитель этого последнего деления (или последний, неравный нулю, остаток) и есть общий наибольший делитель двух данных чисел.

Пример. Даны числа: $r = 76501$, $r_1 = 29719$. Найдем:

$$\begin{aligned}
76501 &= 2 \cdot 29719 + 17063 \\
29719 &= 1 \cdot 17063 + 12656 \\
17063 &= 1 \cdot 12656 + 4407 \\
12656 &= 2 \cdot 4407 + 3842 \\
4407 &= 1 \cdot 3842 + 565 \\
3842 &= 6 \cdot 565 + 452 \\
565 &= 1 \cdot 452 + 113 \\
452 &= 4 \cdot 113
\end{aligned}$$

Таким образом: $D(76501, 29719) = 113$.

Чтобы найти общее наименьшее кратное двух чисел, можно воспользоваться теоремой 12 (§ 5), которая дает:

$$M(r, r_1) = \frac{r \cdot r_1}{D(r, r_1)} = \frac{r}{D(r, r_1)} \cdot r_1 = r \cdot \frac{r_1}{D(r, r_1)}.$$

В предыдущем примере найдем:

$$M(76501, 29719) = \frac{76501 \cdot 29719}{113} = 20119763.$$

Наконец, чтобы найти общий наибольший делитель или общее наименьшее кратное нескольких чисел, можно воспользоваться теоремами 13 и 14 (§ 6).

§ 20. Из формул (16) получим, деля обе части первой на r_1, обе части второй на r_2, третьей — на r_3 и т. д.

$$\begin{aligned}
\frac{r}{r_1} &= q_1 + \frac{r_2}{r_1} \\
\frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2} \\
\frac{r_2}{r_3} &= q_3 + \frac{r_4}{r_3} \\
&\cdots\cdots\cdots \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}} \\
\frac{r_{n-1}}{r_n} &= q_n;
\end{aligned}$$

отсюда:

$$\frac{r}{r_1}=q_1+\frac{1}{\frac{r_1}{r_2}}=q_1+\frac{1}{q_2+\frac{1}{\frac{r_2}{r_3}}}=q_1+\frac{1}{q_2+\frac{1}{q_3+\frac{1}{\frac{r_3}{r_4}}}} \text{ и т. д.}$$

Таким образом, $\frac{r}{r_1}$ представляется так:

$$\frac{r}{r_1}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4+\ddots+\cfrac{1}{q_n}}}}.$$

Правая часть есть так называемая *цепная* (или *непрерывная*) дробь; она состоит из отдельных звеньев: q_1, $+\frac{1}{q_2}$, $+\frac{1}{q_3}$, ... и сокращенно обозначается так:

$$\frac{r}{r_1}=(q_1,\ q_2,\ q_3,\ \ldots\ q_n),$$

$q_1, q_2, q_3, \ldots q_n$ называются *частными знаменателями* цепной дроби.

Таким образом, мы *разлóжили* $\frac{r}{r_1}$ в цепную дробь. Если дана правильная дробь $\frac{r_1}{r}$, то мы, очевидно, получим такое разложение:

$$\frac{r_1}{r}=\frac{1}{\frac{r}{r_1}}=\cfrac{1}{q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_n}}}=(0,q_1,q_2,\ \ldots\ q_n)$$

(в скобках непременно надо писать 0 на первом месте).

Наконец, если дана отрицательная дробь, то ее всегда можно представить так:

$$-k+\frac{r_1}{r},$$

где $k>0$ — целое число, а $\frac{r_1}{r}$ — правильная положительная дробь.

Таким образом:

$$-k+\frac{r_1}{r}=(-k,\ q_1,\ q_2,\ \ldots\ q_n),$$

где все звенья, кроме первого, положительны. Следовательно:

Теорема 33. Всякое рациональное число можно и только одним образом разложить в цепную дробь, в которой все частные знаменатели — целые числа и, начиная со второго, — положительные (первый может быть >0, или <0, или $=0$) и последний — больше единицы.

Замечание 1. Всякое целое число можно рассматривать как цепную дробь, имеющую только одно звено; например: $3 = (3)$. Дробь вида $\frac{1}{a}$ можно рассматривать как цепную дробь с двумя звеньями: $\frac{1}{a} = (0,\ a)$.

Замечание 2. Если не поставлено условие, что последний частный знаменатель $q_n > 1$, то можно данное рациональное число разложить в цепную дробь двумя способами: если один есть $(q_1,\ q_2,\ \ldots\ q_n)$, и $q_n > 1$, то другой: $(q_1,\ q_2,\ \ldots\ q_n - 1,\ 1)$. Здесь число звеньев увеличивается на единицу, и последний частный знаменатель равен единице.

Пример 1. (См. пример § 19).

$$\frac{76501}{29719} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{4}}}}}}} = (2,\ 1,\ 1,\ 2,\ 1,\ 6,\ 1,\ 4).$$

Пример 2. Разложить в цепную дробь число $-\frac{48}{109}$.

Имеем: $$-\frac{48}{109} = -1 + \frac{61}{109}.$$

Находим:

$$\begin{aligned} 109 &= 1 \cdot 61 + 48 \\ 61 &= 1 \cdot 48 + 13 \\ 48 &= 3 \cdot 13 + 9 \\ 13 &= 1 \cdot 9 + 4 \\ 9 &= 2 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 \end{aligned}$$

Следовательно:

$$-\frac{48}{109} = (-1,\ 1,\ 1,\ 3,\ 1,\ 2,\ 4).$$

Возникает обратный вопрос: если дана цепная дробь, то как ее обратить в обычную? Очевидно, что всякая конечная цепная дробь равна некоторому рациональному числу, ибо она является выражением, в котором над данными целыми числами (частными знаменателями) требуется выполнить конечное число рациональных действий. Вычислить конечную цепную дробь не трудно; вычислим, например, цепную дробь в примере 1. Делаем так (с конца):

$$1 + \frac{1}{4} = \frac{5}{4};\ 1 : \frac{5}{4} = \frac{4}{5};\ 6 + \frac{4}{5} = \frac{34}{5};\ 1 : \frac{34}{5} = \frac{5}{34};$$

$$1 + \frac{5}{34} = \frac{39}{34};\ 1 : \frac{39}{34} = \frac{34}{39};\ 2 + \frac{34}{39} = \frac{112}{39};\ 1 : \frac{112}{39} = \frac{39}{112};$$

$$1 + \frac{39}{112} = \frac{151}{112};\ 1 : \frac{151}{112} = \frac{112}{151};\ 1 + \frac{112}{151} = \frac{263}{151};\ 1 : \frac{263}{151} = \frac{151}{263};$$

$$2 + \frac{151}{263} = \frac{677}{263}.$$

Следовательно:

$$(2,\ 1,\ 1,\ 2,\ 1,\ 6,\ 1,\ 4)=\frac{677}{263}.$$

Заметим, что мы получили значение цепной дроби сразу в простейшем виде, как несократимую дробь.

Чтобы получить способы быстрого вычисления цепных дробей, нужно подробнее исследовать их и алгорифм Эвклида, служащий их основою. Эти исследования приведут нас и к важным теоретическим выводам. Мы ими займемся в § 22.

§ 21. Подобно рациональному числу мы можем и иррациональное (вещественное) число разложить в цепную дробь. Для этого нужно только иметь средства выделить целую часть $[x]$ числа x.

Пусть требуется разложить в цепную дробь число α. Находим $[\alpha]=a_1$; тогда $\alpha=a_1+\frac{1}{\alpha_1}$, где $\alpha_1>1$. Далее, находим $[\alpha_1]=a_2$; тогда $\alpha_1=a_2+\frac{1}{\alpha_2}$, где $\alpha_2>1$; следовательно, $\alpha=a_1+\cfrac{1}{a_2+\cfrac{1}{\alpha_3}}$.

Пусть, далее, $[\alpha_2]=a_3$; $\alpha_2=a_3+\frac{1}{\alpha_3}$; $\alpha_3>1$; и т. д. Получаем:

$$\alpha=a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cdots}}=(a_1,\ a_2,\ a_3,\ \ldots).$$

Конечно, при α-иррациональном этот процесс никогда не кончится, и мы получим бесконечную цепную дробь. Здесь возникает вопрос: что же понимать под такою бесконечною дробью? Как определить ее сходимость и как ее приближенно вычислить? Все эти вопросы мы разберем в дальнейших параграфах. Сейчас только заметим, что разложить в цепную дробь можно и неизвестные нам числа α, например, корни алгебраических или трансцендентных уравнений; нужно только уметь выделять целые части корней таких уравнений.

Пример 1. Разложить в цепную дробь $\sqrt{28}$.

Имеем: $\sqrt{28}=5+\frac{1}{\alpha}$; $\alpha>1$.

Отсюда:

$$\alpha=\frac{1}{\sqrt{28}-5}=\frac{\sqrt{28}+5}{3}=3+\frac{1}{\beta};\ \beta>1;$$

$$\beta=\frac{3}{\sqrt{28}-4}=\frac{\sqrt{28}+4}{4}=2+\frac{1}{\gamma};$$

$$\gamma=\frac{4}{\sqrt{28}-4}=\frac{\sqrt{28}+4}{3}=3+\frac{1}{\delta};$$

$$\delta=\frac{3}{\sqrt{28}-5}=\sqrt{28}+5=10+\frac{1}{\alpha},$$

ибо мы уже имели: $\sqrt{28}=5+\frac{1}{\alpha}$. Таким образом, далее повто-

ряются те же самые знаменатели: α, β, γ, δ, и цепная дробь получается *периодическая*. Получим:

$$\sqrt{28} = 5 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{10 + \cfrac{1}{3 + \cfrac{1}{2 + \ddots}}}}}} = (5, (3, 2, 3, 10)).$$

Мы видим, что это дробь *смешанная периодическая;* ее период 3, 2, 3, 10 начинается только со 2-го звена. В дальнейшем мы увидим, что эта периодичность здесь не случайна.

Пример 2. Разложить в цепную дробь положительный корень уравнения:

$$x^4 - x - 1 = 0.$$

Легко видеть, что положительный корень этого уравнения лежит между 1 и 2; следовательно, можно допустить:

$$x = 1 + \frac{1}{y},$$

где $y > 1$.

Разложим левую часть нашего уравнения по степеням $\frac{1}{y} = x - 1$; для этого применим известный из алгебры так называемый *алгорифм Горнера* (Horner):

	1	0	0	—1	—1
1	1	1	1	0	—1
1	1	2	3	3	
1	1	3	6		
1	1	4			

Таким образом, имеем:

$$\frac{1}{y^4} + 4 \cdot \frac{1}{y^3} + 6 \cdot \frac{1}{y^2} + 3 \cdot \frac{1}{y} - 1 = 0,$$

или уравнение для y:

$$y^4 - 3y^3 - 6y^2 - 4y - 1 = 0.$$

Корень этого уравнения лежит между 4 и 5; следовательно, можно взять $y = 4 + \frac{1}{z}$ и разложить левую часть уравнения по степеням $y - 4 = \frac{1}{z}$:

	1	—3	—6	—4	—1
4	1	1	—2	—12	—49
4	1	5	18	60	
4	1	9	54		
4	1	13			

Таким образом, получим уравнение для z:

$$49z^4 - 60z^3 - 54z^2 - 13z - 1 = 0.$$

Это уравнение имеет корень между 1 и 2. Подставляем $z - 1 = \frac{1}{t}$ и вычисляем:

	49	−60	−54	−13	−1
1	49	−11	−65	−78	−79
1	49	38	−27	−105	
1	49	87	60		
1	49	136			

Получаем уравнение для t:

$$79t^4 + 105t^3 - 60t^2 - 136t - 49 = 0.$$

Это уравнение тоже имеет корень между 1 и 2. Берем $t - 1 = \frac{1}{u}$ и вычисляем

	79	105	−60	−136	−49
1	79	184	124	−12	−61
1	79	263	387	375	
1	79	342	729		
1	79	421			

Получаем уравнение для u:

$$61u^4 - 375u^3 - 729u^2 - 421u - 79 = 0,$$

которое имеет корень между 6 и 7 На этом остановимся.

Таким образом, для корня x данного уравнения имеем:

$$x = 1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \ldots}}}}$$

Эта цепная дробь не периодическая.

Способ вычисления корней алгебраических уравнений при помощи цепных дробей принадлежит Лагранжу (Lagrange, XVIII в.).

Пример 3. Разложить в цепную дробь корень показательного уравнения:

$$2^x = 5.$$

Очевидно, что x лежит между 2 и 3; пусть $x = 2 + \frac{1}{y}$; $y > 1$. Имеем:

$$2^{2 + \frac{1}{y}} = 2^2 \cdot 2^{\frac{1}{y}} = 5;$$

$$2^{\frac{1}{y}} = \frac{5}{4}; \quad \left(\frac{5}{4}\right)^y = 2;$$

испытаниями находим, что y лежит между 3 и 4; следовательно,

$$y = 3 + \frac{1}{z},$$

где $z > 1$.

Получаем:

$$\left(\frac{5}{4}\right)^{3+\frac{1}{z}} = 2; \quad \frac{125}{64} \cdot \left(\frac{5}{4}\right)^{\frac{1}{z}} = 2; \quad \left(\frac{5}{4}\right)^{\frac{1}{z}} = \frac{128}{125};$$

$$\left(\frac{128}{125}\right)^{z} = \frac{5}{4} \text{ или } (1{,}024)^{z} = 1{,}25.$$

Испытаниями найдем, что z лежит между 9 и 10. Таким образом, получаем:

$$x = \lg_2 5 = 2 + \cfrac{1}{3 + \cfrac{1}{9 + \ldots}}$$

Так мы можем приближенно вычислять логарифмы при помощи цепных дробей; но этот способ весьма неудобен вследствие больших вычислений

§ 22. Алгорифм Эйлера. Обобщим теперь алгорифм Эвклида следующим образом: пусть r и r_1 — два данных числа, а $k_1, k_2, \ldots k_n$ — какие-нибудь n постоянных или переменных величин (мы будем считать их целыми положительными числами, но все наши дальнейшие алгебраические выводы остаются правильными, если числа $r, r_1, k_1, k_2, \ldots k_n$ — любые, не только целые положительные). Найдем теперь числа $r_2, r_3, \ldots r_n, r_{n+1}$ из следующих уравнений:

$$\left.\begin{aligned} r &= k_1 r_1 + r_2 \\ r_1 &= k_2 r_2 + r_3 \\ &\ldots\ldots\ldots\ldots \\ r_{m-1} &= k_m r_m + r_{m+1} \\ r_m &= k_{m+1} r_{m+1} + r_{m+2} \\ &\ldots\ldots\ldots\ldots \\ r_{n-1} &= k_n r_n + r_{n+1} \end{aligned}\right\} \qquad (17)$$

Эти уравнения (17) отличаются от уравнений (16) только тем, что здесь $k_1, k_2, \ldots k_n$ — не частные от делений r на r_1, r_1 на r_2 и т. д., как в (16) $q_1, q_2, \ldots q_n$. Нахождение чисел $r_2, r_3, \ldots r_{n+1}$ при данных r, r_1 и k_λ и есть алгорифм Эйлера. Очевидно, что алгорифм Эвклида — частный случай алгорифма Эйлера, поэтому все следствия из последнего остаются верными и для первого. Очевидно также, что в алгорифме Эйлера мы можем остановиться на любом из уравнений (17), т. е. каждое из них считать последним.

Но мы можем каждое из уравнений (17) считать и первым, например, уравнение $r_m = k_{m+1} r_{m+1} + r_{m+2}$, рассматривая r_m и r_{m+1} как данные числа вместо r и r_1. Отсюда далее найдем $r_{m+2}, \ldots r_{n+1}$.

Легко видеть, что и предыдущие $r_\lambda : r_{m-1}, r_{m-2}, \dots r_1, r$ определяются через r_m и r_{m+1}; вообще, все числа r_λ однозначно определяются через любые два соседние из них. Найдем, как выражается r через r_m, r_{m+1}. Имеем:

$$r = k_1 r_1 + r_2 = k_1(k_2 r_2 + r_3) + r_2 = (k_1 k_2 + 1) r_2 + k_1 r_3.$$

Подставляя вместо r_2 его выражение $k_3 r_3 + r_4$, найдем r в зависимости от r_3 и r_4 и т. д. Мы видим, что r — линейная однородная функция от r_m и r_{m+1}, коэффициенты которой — целые функции от $k_1, k_2, \dots k_m$. Обозначим:

$$r = Gr_m + Hr_{m+1} \tag{18}$$

и подставим сюда вместо r_m его выражение $k_{m+1} r_{m+1} + r_{m+2}$. Тогда найдем r в зависимости от r_{m+1} и r_{m+2}:

$$r = (Gk_{m+1} + H) r_{m+1} + Gr_{m+2}. \tag{19}$$

Но m — любой индекс из ряда 1, 2, ... n. Назовем G в уравнении (18) *первым*, а H в (18) *вторым* коэффициентом, (18) — *предыдущим*, (19) — *последующим* уравнением. Из уравнений (18) и (19) выводим такие общие заключения:

1. Второй коэффициент последующего уравнения равен первому коэффициенту предыдущего уравнения.

2. Первый коэффициент последующего уравнения определяется через коэффициенты предыдущего уравнения как такое выражение:

$$Gk_{m+1} + H. \tag{20}$$

Мы видим, что этот коэффициент зависит от k_{m+1}, следовательно, G, как первый коэффициент предыдущего уравнения, зависит от k_m, тогда как H — первый коэффициент уравнения, предыдущего уравнению (18) — не зависит от k_m, но зависит от k_{m-1}. Таким образом, вообще G зависит от $k_1, k_2, \dots k_m$. Мы обозначим:

$$G = [k_1, k_2, \dots k_m]$$

и назовем этот символ *скобками Эйлера*. Это — некоторая целая рациональная функция от $k_1, k_2, \dots k_m$. При таком обозначении уравнение (18) примет вид:

$$r = [k_1, k_2, \dots k_m] r_m + [k_1, k_2, \dots k_{m-1}] r_{m+1}, \tag{21}$$

ибо H, как первый коэффициент уравнения, предыдущего по отношению к уравнению (18), следует обозначить через $[k_1, k_2, \dots k_{m-1}]$. Далее, выражение (20) дает такую *рекуррентную формулу*:

$$[k_1, k_2, \dots k_{m+1}] = [k_1, k_2, \dots k_m] k_{m+1} + [k_1, k_2, \dots k_{m-1}]. \tag{22}$$

Эта формула дает возможность постепенного вычисления скобок Эйлера, если только нам известны эти скобки с одним и с двумя аргументами. Но ведь мы имеем: $r = (k_1 k_2 + 1) r_2 + k_1 r_3$; это дает

$$[k_1] = k_1; \; [k_1, k_2] = k_1 k_2 + 1. \tag{23}$$

Пример. Вычислить [3, 1, 2, 4, 1, 2]. Вычисляем последовательно: $[3] = 3$; $[3,1] = 3 \cdot 1 + 1 = 4$; $[3, 1, 2] = 4 \cdot 2 + 3 = 11$; $[3, 1, 2, 4] = 11 \cdot 4 + 4 = 48$; $[3, 1, 2, 4, 1] = 48 \cdot 1 + 11 = 59$; $[3, 1, 2, 4, 1, 2] = 59 \cdot 2 + 48 = 166$.

Обычно вычисления располагают так: в первой строке пишут числа, данные в скобках: 3, 1, 2, 4, 1, 2; во второй строке слева пишут число 1; под первым числом первой строки (у нас 3) пишут то же число (3); далее, его умножают на следующее число первой строки (1) и к произведению прибавляют предыдущее число 2-й строки (1); результат (4) пишут под вторым числом 1-й строки; этот результат умножают на следующее число 1-й строки (2) и прибавляют предыдущее число 2-й строки (3); результат пишут под следующим числом 1-й строки и т. д.:

	3	1	2	4	1	2
1	3	4	11	48	59	166

§ 23. Считая за первое число не r, а r_1, имеем аналогично (21):

$$r_1 = [k_2, k_3, \dots k_m] r_m + [k_2, k_3, \dots k_{m-1}] r_{m+1}. \qquad (24)$$

Так же получаем и для r_2:

$$r_2 = [k_3, \dots k_m] r_m + [k_3, \dots k_{m-1}] r_{m+1}. \qquad (25)$$

Подставляя выражения для r_1 и r_2 из (24) и (25) в первое уравнение (17), получим

$$r = \{k_1 [k_2, \dots k_m] + [k_3, \dots k_m]\} r_m + \{k_1 [k_2, \dots k_{m-1}] + [k_3, \dots k_{m-1}]\} r_{m+1}. \qquad (26)$$

Но r_m и r_{m+1} можно считать независимыми переменными; следовательно, r только одним образом представляется как линейная однородная функция от r_m и r_{m+1}. Таким образом, сравнивая (26) с (21), получим:

$$[k_1, k_2, \dots k_m] = k_1 [k_2, \dots k_m] + [k_3, \dots k_m]. \qquad (27)$$

Эта формула позволяет вычислять скобки Эйлера «с конца» — сначала $[k_m]$, затем $[k_{m-1}, k_n]$ и т. д. Но $[k_m] = k_m$, $[k_{m-1}, k_m] = k_{m-1}k_m + 1$. Далее, по формуле (27) вычисление идет так же, как и по формуле (22); иными словами, мы вычисляем $[k_1, \dots k_m]$ по (27) так же, как $[k_m, \dots k_1]$ по (22); а это означает, что:

$$[k_1, \dots k_m] = [k_m, \dots k_1]. \qquad (28)$$

Это — важное свойство скобок Эйлера.

Замечание. Формула (27) не имеет смысла при $m = 2$, ибо в этом случае скобок $[k_3, \dots k_m]$ не существует. Условились считать, что в этом случае мы имеем «пустые» скобки Эйлера, которые равны 1. Тогда формула (27) остается верной и в этом случае,— она просто совпадает со второй формулой (23).

Имеем далее (аналогично с (21)):

$$r_m = [k_{m+1}, \ldots k_n] r_n + [k_{m+1}, \ldots k_{n-1}] r_{n+1};$$
$$r_{m+1} = [k_{m+2}, \ldots k_n] r_n + [k_{m+2}, \ldots k_{n-1}] r_{n+1}.$$

Подставляя эти значения в (21), получим:

$$r = \{[k_1, \ldots k_m][k_{m+1}, \ldots k_n] + [k_1, \ldots k_{m-1}][k_{m+2}, \ldots k_n]\} r_n + \\ + \{[k_1, \ldots k_m][k_{m+1}, \ldots k_{n-1}] + [k_1, \ldots k_{m-1}][k_{m+2}, \ldots k_{n-1}]\} r_{n+1}.$$

С другой стороны, формула (21) непосредственно дает (при $m = n$):

$$r = [k_1, \ldots k_n] r_n + [k_1, \ldots k_{n-1}] r_{n+1}.$$

Из двух последних равенств выводим (так как r_n и r_{n+1} независимы):

$$[k_1, \ldots k_n] = [k_1, \ldots k_m][k_{m+1}, \ldots k_n] + \\ + [k_1, \ldots k_{m-1}][k_{m+2}, \ldots k_n]. \tag{29}$$

Здесь m — какое-нибудь (целое) число между 1 и n. Эта формула является обобщением формул (22) и (27).

Из формул (17) получаем непосредственно (начав с конца):

$$\left.\begin{aligned} r_{n+1} &= -k_n r_n + r_{n-1} \\ r_n &= -k_{n-1} r_{n-1} + r_{n-2} \\ &\ldots\ldots\ldots\ldots \\ r_2 &= -k_1 r_1 + r. \end{aligned}\right\} \tag{30}$$

Эти уравнения того же типа, что и (17), и только знаками у k_λ отличаются от (17); следовательно, все формулы, полученные нами для скобок Эйлера, остаются правильными и для (30), если заменить k_λ через $-k_\lambda$. Но мы имеем:

$$[-k_n] = -[k_n];\ [-k_n, -k_{n-1}] = (-k_n)(-k_{n-1}) + 1 = \\ = k_n k_{n-1} + 1 = [k_n, k_{n-1}].$$

Пусть доказано, что:

$$[-k_1, -k_2, \ldots -k_m] = (-1)^m \cdot [k_1, k_2, \ldots k_m]; \tag{31}$$

тогда (22) дает:

$$[-k_1, -k_2, \ldots -k_{m+1}] = [-k_1, \ldots -k_m](-k_{m+1}) + \\ + [-k_1, \ldots -k_{m-1}] = (-1)^m [k_1, \ldots k_m](-k_{m+1}) + \\ + (-1)^{m-1}[k_1, \ldots k_{m-1}] = (-1)^{m+1} \cdot \{[k_1, \ldots k_m] k_{m+1} + \\ + [k_1, \ldots k_{m-1}]\} = (-1)^{m+1} \cdot [k_1, k_2, \ldots k_{m+1}],$$

и формула (31) доказана для всякого m.

Исходя теперь из формул (30), определим r_n по формуле (21) в зависимости от r_1 и r:

$$r_n = [-k_{n-1}, \ldots -k_1] r_1 + [-k_{n-1}, \ldots -k_2] r;$$

или, согласно формулам (31) и (28):

$$r_n = (-1)^{n-1}[k_1, \ldots k_{n-1}] r_1 + (-1)^n [k_2, \ldots k_{n-1}] r. \tag{32}$$

Подставляя сюда выражения для r и r_1 через r_n и r_{n+1} по формулам (17) и сравнивая коэффициенты при r_n в обеих частях полученного тождества, найдем:

$$(-1)^{n-1}[k_1, \dots k_{n-1}][k_2, \dots k_n] + \\ + (-1)^n [k_2, \dots k_{n-1}][k_1, \dots k_n] = 1,$$

или:

$$[k_1, \dots k_n][k_2, \dots k_{n-1}] - [k_1, \dots k_{n-1}][k_2, \dots k_n] = (-1)^n. \quad (33)$$

§ 24. Если числа $k_1, k_2, \dots k_n$ все целые положительные, то очевидно, что и скобки Эйлера $[k_1, k_2, \dots k_n]$ — целое положительное число; при этом $[k_1, \dots k_m] > [k_2, \dots k_m] > [k_3, \dots k_m]$. Следовательно, формула (27) при $m = n$ показывает, что k_1 — частное, а $[k_3, \dots k_n]$ — остаток от деления $[k_1, \dots k_n]$ на $[k_2, \dots k_n]$.

Подобно же, k_2 — частное, а $[k_4, \dots k_n]$ — остаток от деления $[k_2, \dots k_n]$ на $[k_3, \dots k_n]$ и т. д. Если мы возьмем $r = [k_1, \dots k_n]$, $r_1 = [k_2, \dots k_n]$, то по (27) получим: $r_2 = [k_3, \dots k_n]$ и далее так же: $r_3 = [k_1, \dots k_n]$, $\dots$ $r_{n-2} = [k_{n-1}, k_n]$, $r_{n-1} = [k_n] = k_n$, а далее: $r_n = 1$, $r_{n+1} = 0$. И алгорифм Эйлера совпадает с алгорифмом Эвклида, причем $r_n = D(r, r_1)$. По формуле (33) получаем, что $r = [k_1, \dots k_n]$ и $r_1 = [k_2, \dots k_n]$ взаимно-простые, поэтому и получается $r_n = 1$.

Итак:

Теорема 34. Всякие n целых положительных чисел $k_1, k_2, \dots k_n$ можно рассматривать как неполные частные в алгорифме Эвклида, примененном к числам $[k_1, \dots k_n]$ и $[k_2, \dots k_n]$.

Эта теорема не дает нам ничего принципиально нового: она показывает только, что всякую конечную цепную дробь (с целыми положительными частными знаменателями) можно всегда обратить в обыкновенную дробь. Действительно, формула (27) дает:

$$\frac{[k_1, \dots k_n]}{[k_2, \dots k_n]} = k_1 + \frac{[k_3, \dots k_n]}{[k_2, \dots k_n]} = k_1 + \frac{1}{\frac{[k_2, \dots k_n]}{[k_3, \dots k_n]}};$$

но так же найдем

$$\frac{[k_2, \dots k_n]}{[k_3, \dots k_n]} = k_2 + \frac{1}{\frac{[k_3, \dots k_n]}{[k_4, \dots k_n]}}$$

и т. д.

Таким образом:

$$\frac{[k_1, \dots k_n]}{[k_2, \dots k_n]} = k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \ddots + \cfrac{1}{k_n}}} = (k_1, k_2, \dots k_n) \quad (34)$$

Это дает способ вычисления цепных дробей.

Пример 1. Вычислить дробь (3, 5, 1, 1, 2). Пишем данные

частные знаменатели в обратном порядке и вычисляем скобки Эйлера (способом, данным в конце § 22):

$$\begin{array}{c|ccccc} & 2 & 1 & 1 & 5 & 3 \\ \hline 1 & 2 & 3 & 5 & 28 & 89 \end{array}.$$

Последнее из полученных чисел будет числителем, а предпоследнее — знаменателем нашей дроби. Итак:

$$(3,\ 5,\ 1,\ 1,\ 2) = \frac{89}{28}.$$

Действительно, мы имеем:

$$89 = [2,\ 1,\ 1,\ 5,\ 3] = [3,\ 5,\ 1,\ 1,\ 2];$$

$28 = [2,\ 1,\ 1,\ 5] = [5,\ 1,\ 1,\ 2]$ (см. формулу (28)).

Пример 2. Вычислить:

$$\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{4}}}}$$

Здесь имеем:

$$\begin{array}{c|ccccc} & 4 & 3 & 2 & 2 & 0 \\ \hline 1 & 4 & 13 & 30 & 73 & 30 \end{array}.$$

Следовательно:

$$(0,\ 2,\ 2,\ 3,\ 4) = \frac{30}{73}.$$

Замечание. Заметим, что этот способ вычисления цепных дробей — просто упорядоченный элементарный способ, о котором мы упоминали в конце § 20. Но это упорядочение дало нам определенный метод быстрого вычисления цепных дробей.

Как уже было сказано, можно прекратить алгорифм Эйлера на каком угодно из уравнений (17), хотя бы на m-м $(m < n)$; тогда получим по (34)

$$\frac{[k_1, \ldots k_m]}{[k_2, \ldots k_m]} = k_1 + \cfrac{1}{k_2 + \cdots + \cfrac{1}{k_m}} \qquad (35)$$

В правой части (35) мы имеем только часть нашей цепной дроби (34), а именно, m первых ее звеньев. Числовое значение этой части, т. е. дробь $\frac{[k_1, \ldots k_m]}{[k_2, \ldots k_m]}$ называется m-ой *подходящей дробью* данной цепной дроби. При $m = 1, 2, \ldots n$ мы получаем первую, вторую и т. д. подходящие дроби. Вычисляя скобки Эйлера $[k_1, \ldots k_n]$ и $[k_2, \ldots k_n]$, мы получаем последовательно числители и знаменатели всех подходящих дробей нашей цепной дроби. Но для этого следует эти две скобки вычислять отдельно,— нельзя применить формулу (28).

Вернемся опять к нашим примерам 1 и 2 и вычислим там все подходящие дроби. Для дроби (3, 5, 1, 1, 2):

	3	5	1	1	2
1	3	16	19	35	89
	1	5	6	11	28

Во второй строке этой таблицы — числители, а в третьей — знаменатели подходящих дробей. Третья строка строится точно так же, как и вторая (при использовании первой строки), только начиная со второго числа (с 5). Таким образом, подходящие дроби следующие:

$$\frac{3}{1},\ \frac{16}{5},\ \frac{19}{6},\ \frac{35}{11},\ \frac{89}{28}.$$

Для дроби (0, 2, 2, 3, 4):

	0	2	2	3	4
1	0	1	2	7	30
	1	2	5	17	73

И подходящие дроби: $0,\ \frac{1}{2},\ \frac{2}{5},\ \frac{7}{17},\ \frac{30}{73}$.

Обозначим $p_m = [k_1, k_2, \ldots k_m]$, $q_m = [k_2, \ldots k_m]$; тогда m-я подходящая дробь будет $\frac{p_m}{q_m}$. Но формула (33) дает (если заменить там n через m)

$$p_m q_{m-1} - p_{m-1} q_m = (-1)^m. \qquad (36)$$

Из этой формулы видно, что p_m и q_m взаимно-простые, т. е. подходящие дроби $\frac{p_m}{q_m}$ несократимы. Деля (36) на $q_{m-1}q_m$, получим:

$$\frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}} = \frac{(-1)^m}{q_{m-1}q_m}. \qquad (37)$$

Таким образом, абсолютная величина разности двух соседних подходящих дробей уменьшается с возрастанием m (ибо и q_m возрастает), а знаки этих разностей попеременно $+$ и $-$. Мы докажем следующее:

Теорема 35. Точное значение цепной дроби всегда находится между двумя соседними подходящими дробями, причем оно ближе к последующей, чем к предыдущей подходящей дроби.

Доказательство. Пусть дана цепная дробь

$$x = k_1 + \cfrac{1}{k_2 + \ddots + \cfrac{1}{k_m + \cfrac{1}{k_{m+1} + \ddots + \cfrac{1}{k_n}}}}$$

Обозначим: $y = k_{m+1} + \cfrac{1}{k_{m+2} + \ddots + \cfrac{1}{k_n}}$;

тогда: $x = k_1 + \frac{1}{k_2} + \cdot \cdot \cdot + \cfrac{1}{k_m + \frac{1}{y}}$

и мы имеем:

$$x = \frac{p_m y + p_{m-1}}{q_m y + q_{m-1}},$$

ибо x $(m+1)$-я подходящая дробь, если считать y последним частным знаменателем (см. формулу (22)). Отсюда имеем:

$$xq_m y + xq_{m-1} = p_m y + p_{m-1};$$
$$y(xq_m - p_m) = p_{m-1} - xq_{m-1};$$
$$yq_m\left(x - \frac{p_m}{q_m}\right) = q_{m-1}\left(\frac{p_{m-1}}{q_{m-1}} - x\right); \quad (38)$$

но $y > 1$, $q_m > q_{m-1} > 0$, т. е. $yq_m > q_{m-1}$; из (38) получаем: $\left|x - \frac{p_m}{q_m}\right| < \left|\frac{p_{m-1}}{q_{m-1}} - x\right|$, и знаки у $x - \frac{p_m}{q_m}$ и $\frac{p_{m-1}}{q_{m-1}} - x$ одинаковы. Это и доказывает нашу теорему.

Отсюда имеем на основании формулы (37):

$$\left|x - \frac{p_m}{q_m}\right| < \left|\frac{p_{m+1}}{q_{m+1}} - \frac{p_m}{q_m}\right| = \frac{1}{q_m q_{m+1}}. \quad (39)$$

Эта формула дает верхний предел погрешности приближенного значения $\frac{p_m}{q_m}$ для x. Мы видим, что $\frac{p_m}{q_m}$ с возрастанием m действительно все более подходит к x; отсюда и название: подходящая дробь.

Имеем:

$$q_{m+1} = q_m k_{m+1} + q_{m-1} \geqq q_m + q_{m-1} > q_m.$$

Следовательно:

$$\frac{1}{q_m q_{m+1}} \leqq \frac{1}{q_m(q_m + q_{m-1})} < \frac{1}{q_m^2}.$$

Таким образом, в правой части (39) вместо $\frac{1}{q_m q_{m+1}}$ можно взять $\frac{1}{q_m(q_m + q_{m-1})}$ или $\frac{1}{q_m^2}$, как верхние пределы нашей погрешности; они хотя и не так точны, как $\frac{1}{q_m q_{m+1}}$, но более простые.

Итак:

Теорема 36. Если вместо точного значения цепной дроби взять ее m-ю подходящую дробь, то за верхний предел погрешности можно принять:

$$\frac{1}{q_m q_{m+1}}, \quad \text{или} \quad \frac{1}{q_m(q_m + q_{m-1})}, \quad \text{или} \quad \frac{1}{q_m^2}.$$

§ 25. Пусть теперь нам дана бесконечная цепная дробь, т. е. бесчисленное множество (бесконечная последовательность) частных

знаменателей $k_1, k_2, k_3, \ldots$; обозначим ее $(k_1, k_2, k_3, \ldots)$. Пусть при этом все k_λ — целые положительные числа. Тогда можно построить бесчисленное множество подходящих дробей $\frac{p_m}{q_m}$; но формула (37) остается верною, ибо для ее вывода нужны только m первых звеньев цепной дроби. Очевидно, что при беспредельном возрастании m q_m (а также и q_{m+1}) тоже беспредельно возрастает, ибо все k_m — целые положительные числа; следовательно:

$$\lim_{m \to \infty} \left(\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}}\right) = 0. \tag{40}$$

С другой стороны, та же формула (37) дает:

$$\frac{p_{2m}}{q_{2m}} - \frac{p_{2m-1}}{q_{2m-1}} > \frac{p_{2m}}{q_{2m}} - \frac{p_{2m+1}}{q_{2m+1}} > \frac{p_{2m+2}}{q_{2m+2}} - \frac{p_{2m+1}}{q_{2m+1}} > 0,$$

ибо $q_{2m-1}q_{2m} < q_{2m}q_{2m+1} < q_{2m+1}q_{2m+2}$; следовательно:

$$\frac{p_{2m-1}}{q_{2m-1}} < \frac{p_{2m+1}}{q_{2m+1}}; \quad \frac{p_{2m}}{q_{2m}} > \frac{p_{2m+2}}{q_{2m+2}}.$$

Таким образом, мы имеем два ряда дробей:

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \frac{p_5}{q_5} < \ldots; \quad \frac{p_2}{q_2} > \frac{p_4}{q_4} > \frac{p_6}{q_6} > \ldots;$$

числа первого ряда возрастают, числа второго ряда убывают. Из формулы (37) следует, что числа первого ряда остаются меньше соответственных чисел второго ряда; следовательно, числа первого и числа второго ряда стремятся к пределам. Из формулы (40) следует, что эти пределы равны; значит, существует единый предел ряда подходящих дробей:

$$x = \lim_{m \to \infty} \frac{p_m}{q_m}.$$

Определение. Этот предел ряда подходящих дробей мы и определяем как значение бесконечной цепной дроби:

$$x = (k_1, k_2, k_3, \ldots).$$

Теоремы 35 и 36 непосредственно обобщаются на случаи бесконечных цепных дробей, ибо доказательства их совсем не требуют чтобы цепная дробь была конечна,— требуется только, чтобы она имела определенное значение.

Таким образом, бесконечная цепная дробь (с целыми положительными частными знаменателями) всегда сходящаяся; ее легко вычислить с какой угодно точностью. Пусть погрешность должна быть $< \varepsilon$; вычисляем последовательные подходящие дроби $\frac{p_m}{q_m}$, пока (при некотором определенном m) не получим, что $q_m^2 > \varepsilon^{-1}$. В таком случае соответственная дробь $\frac{p_m}{q_m}$ и есть приближенное значение цепной дроби с точностью до ε,— с недостатком при m нечетном и с избытком при m четном.

Для иллюстрации вернемся к примерам 1, 2, 3 § 22.

1. Мы имеем: $\sqrt{28} = (5, (3, 2, 3, 10))$; пусть требуется вычислить $\sqrt{28}$ с точностью до 0,0001. Составляем таблицу:

	5	3	2	3	10	3	2 ...
1	5	16	37	127	1307		
	1	3	7	24	247		

Остановимся на $\frac{1307}{247}$, ибо $247^2 > 10000$; следовательно, $\frac{1307}{247}$ и есть $\sqrt{28}$ с точностью до 0,0001 с недостатком, ибо это — пятая подходящая дробь, т. е. с нечетным номером. Обратим $\frac{1307}{247}$ в десятичную дробь, т. е. разделим 1307 на 247, беря 4 десятичных знака; эту десятичную дробь мы должны взять с избытком. Итак: $\sqrt{28} \approx 5{,}2315$; но мы не знаем, будет ли это значение для корня с избытком или с недостатком.

2. Для положительного корня уравнения $x^4 - x - 1 = 0$ мы нашли цепную дробь: $x = (1, 4, 1, 1, 6, \ldots)$. Мы можем здесь найти пятую подходящую дробь:

	1	4	1	1	6
1	1	5	6	11	72
	1	4	5	9	59

$59^2 > 1000$, следовательно, $\frac{72}{59}$ дает корень нашего уравнения с точностью до 0,001 тоже с недостатком. Обратив $\frac{72}{59}$ в десятичную дробь, получим $x \approx \frac{72}{59} \approx 1{,}221$; но мы не знаем, с избытком ли это или с недостатком.

3. Мы имели: $\lg_2 5 = (2, 3, 9, \ldots)$; находим:

	2	3	9
1	2	7	65
	1	3	28

$28^2 > 100$; следовательно, $\lg_2 5 \approx \frac{65}{28} \approx 2{,}33$ — с точностью до 0,01, но неизвестно, с избытком или с недостатком.

Теорема 37. Если x — точное значение цепной (конечной или бесконечной) дроби, а $\frac{a}{b}$ ее приближенное значение, которое ближе к x, чем подходящая дробь $\frac{p_m}{q_m}$, то $b > q_m$.

Доказательство. При данных условиях и по теореме 35 $\frac{a}{b}$ ближе к $\frac{p_{m+1}}{q_{m+1}}$, чем $\frac{p_m}{q_m}$; следовательно:

$$\left|\frac{a}{b} - \frac{p_{m+1}}{q_{m+1}}\right| < \left|\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}}\right|.$$

Но правая часть по (37) равна $\frac{1}{q_m q_{m+1}}$; следовательно:

$$\frac{|aq_{m+1} - bp_{m+1}|}{bq_{m+1}} < \frac{1}{q_m q_{m+1}}.$$

Пусть $b \leqq q_m$, а следовательно: $bq_{m+1} \leqq q_m q_{m+1}$; отсюда:

$$|aq_{m+1} - bp_{m+1}| < 1.$$

Но левая часть здесь — целое число $\geqq 0$; следовательно:

$$aq_{m+1} - bp_{m+1} = 0,$$

т. е. $\frac{a}{b} = \frac{p_{m+1}}{q_{m+1}}$.

Здесь правая часть — несократимая дробь; следовательно, $b \geqq q_{m+1} > q_m$, что противоречит нашему предположению: $b \leqq q_m$. Этим теорема доказана.

Эта теорема имеет большое значение; она доказывает, что подходящие дроби — наилучшие приближения к данному числу x, т. е. наиболее простые приближения с данной точностью или наиболее точные приближения со знаменателем, не превышающим данного предела. В приложениях математики вообще употребляют десятичные дроби, посредством которых приближенно выражают величины. Но есть вопросы, в которых приходится применять простые дроби для приближенных выражений величин. В таких случаях именно подходящие дроби и являются наиболее простыми и точными.

§ 26. Некоторые применения цепных дробей. 1. Зубчатые колеса. Пусть требуется соединить два вала зубчатыми колесами так, чтобы отношение их угловых скоростей равнялось данному числу α. Угловые скорости колес обратно-пропорциональны числам зубцов; значит, обратное отношение чисел зубцов равно α. Но числа зубцов — целые и не очень большие, тогда как α может быть и иррациональным Следовательно, нашу задачу можно решить только приближенно, взяв для α приближенное значение в форме простой дроби с не очень большим знаменателем. Из предыдущего вытекает, что наиболее выгодно взять одну из подходящих дробей цепной дроби, в которую раскладывается число α.

2. Календарный стиль. Из астрономии известно, что год имеет 365,24220... так называемых «средних» суток. Конечно, такое сложное отношение года к суткам в практической жизни совершенно неудобно; нужно заменить его более простым, хотя бы и менее точным. Разложив 365,24220. . . в цепную дробь, получим:

$$365{,}24220\ldots = 365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{3 + \ldots}}}}$$

Первые подходящие дроби здесь будут:

$$365; \ 365\frac{1}{4}; \ 365\frac{7}{29}; \ 365\frac{8}{33}.$$

Приближение $365\frac{1}{4}$ было известно еще древним народам (египтянам, ассиро-вавилонянам, китайцам), хотя они не имели регулярных високосных годов. 7-го марта 238 года до нашей эры вышел Канопский декрет Птоломея Эвергета, которым предписывалось, чтобы каждый четвертый год имел не 365, а 366 суток. Но через 40 лет этот декрет был забыт, и только в 47 году до н. э. Юлий Цезарь, при участии Сосигена, возобновил его, вставив в каждом четвертом году лишний день в феврале. Этот день назвали bissextilis, откуда происходит и наше название «високосный» год. Это — так называемый старый, или Юлианский стиль.

Новый, или Григорианский стиль дает приближение $365\frac{97}{400}$; оно немного больше, чем $365\frac{7}{29}$ и $365\frac{8}{33}$. Этот стиль отличается от Юлианского тем, что в нем каждый сотый год — не високосный, кроме тех, число сотен которых делится без остатка на 4. Так, 1700-й, 1800-й, 1900-й годы — не високосные, тогда как 1600-й, 2000-й годы — високосные, т. е. 400 лет имеют 97 лишних суток, а не 100 суток, как в Юлианском стиле.

Уже в XV столетии было замечено отставание Юлианского стиля (тогда на 10 суток) и были предложения реформировать календарь. Но эта реформа была проведена только в конце XVI столетия. В католических странах она была осуществлена буллою папы Григория XIII от 1 марта 1582 года. 10 суток — с 5-го по 14 октября были вычеркнуты, т. е. вместо 5-го сразу было велено считать 15 октября 1582 г.

Наиболее точный календарь ввел в Персии в 1079 году персидский астроном и математик (он же и поэт) Омар Альхайями. Он взел цикл из 33 лет, в котором семь раз високосный год считался четвертый, а восьмой раз високосный год был не четвертый, а пятый. Таким образом, здесь имеется 8 лишних суток в 33 года, т. е. для каждого года $365\frac{8}{33}$ суток; это как раз четвертая подходящая дробь.

§ 27. В примере 1 § 21 мы видели, что $\sqrt{28}$ раскладывается в периодическую цепную дробь. Докажем теперь, что вообще $\sqrt{a}$, где a — целое положительное число, раскладывается всегда в периодическую цепную дробь. Пусть $[\sqrt{a}] = k_0$ (целая часть корня), $\sqrt{a} = k_0 + \frac{1}{x_1}$; $x_1 > 1$; имеем:

$$x_1 = \frac{1}{\sqrt{a} - k_0} = \frac{\sqrt{a} + k_0}{a - k_0^2},$$

Обозначим: $k_0 = p_1$, $a - k_0^2 = q_1$; тогда: $0 < p_1 < \sqrt{a}$; $q_1 > 0$; p_1 и q_1 — целые числа; $q_1 < \sqrt{a} + p_1$, ибо $x_1 > 1$;

$$x_1 = \frac{\sqrt{a} + p_1}{q_1} = k_1 + \frac{1}{x_2}; \ k_1 = [x_1]; \ x_2 > 1.$$

Аналогично имеем:

$$x_2 = \frac{\sqrt{a} + p_2}{q_2} = k_2 + \frac{1}{x_3}; \ k_2 = [x_2]; \ x_3 > 1.$$

И вообще:

$$x_m = \frac{\sqrt{a} + p_m}{q_m} = k_m + \frac{1}{x_{m+1}}; \ k_m = [x_m]; \ x_{m+1} > 1.$$

Докажем, что p_m и q_m при всех m — целые положительные числа. Мы видели, что это верно для p_1, q_1; пусть это уже доказано для p_λ, q_λ при всех $\lambda \leqq m$. Имеем:

$$x_{m+1} = \frac{\sqrt{a} + (k_m q_m - p_m)}{[a - (k_m q_m - p_m)^2] : q_m};$$

следовательно:

$$p_{m+1} = k_m q_m - p_m; \ q_{m+1} = \frac{a - (k_m q_m - p_m)^2}{q_m} = \frac{a - p_{m+1}^2}{q_m}; \qquad (41)$$

отсюда:

$$a = p_{m+1}^2 + q_m q_{m+1}.$$

Но заменив m на $m - 1$, мы так же получим:

$$a = p_m^2 + q_{m-1} q_m;$$

следовательно:

$$p_m^2 + q_{m-1} q_m = p_{m+1}^2 + q_m q_{m+1} = (k_m q_m - p_m)^2 + q_m q_{m+1};$$

отсюда

$$p_m^2 + q_{m-1} q_m = k_m^2 q_m^2 - 2k_m p_m q_m + p_m^2 + q_m q_{m+1},$$

или, сократив на p_m^2 и на q_m:

$$q_{m+1} = q_{m-1} + 2k_m p_m - k_m^2 q_m. \qquad (42)$$

Из первой формулы (41) и из формулы (42) видно, что p_{m+1} и q_{m+1} тоже целые числа.

Далее, имеем:

$$x_m - k_m = \frac{\sqrt{a} + p_m}{q_m} - k_m > 0; \ q_m > 0;$$

следовательно:

$$\sqrt{a} + p_m - k_m q_m > 0. \qquad (43)$$

С другой стороны: $a = p_m^2 + q_{m-1} q_m > p_m^2$, т. е. $\sqrt{a} > p_m$; $\sqrt{a} - p_m > 0$;

$$\sqrt{a} - p_m + k_m q_m > 0. \qquad (44)$$

Перемножив (43) и (44) и приняв во внимание первую формулу (41), найдем:

$$a-(k_m q_m - p_m)^2 = a - p_{m+1}^2 > 0,$$

а отсюда по второй формуле (41) получим:

$$q_{m+1} > 0.$$

Пусть $p_{m+1} = k_m q_m - p_m \leqq 0$; тогда: $q_m \leqq k_m p_m \leqq p_m < \sqrt{a}$; следовательно:

$$k_m = \left[\frac{\sqrt{a}+p_m}{q_m}\right] > \left[\frac{k_m q_m + q_m}{q_m}\right] = k_m + 1,$$

т. е. мы пришли к противоречию; значит, $p_{m+1} > 0$.

Итак, p_m и q_m для всякого m — целые положительные числа. Мы имеем:

$$0 < p_m < \sqrt{a};\ 0 < q_m < \sqrt{a} + p_m < 2\sqrt{a}. \qquad (45)$$

ибо $x_m = \frac{\sqrt{a}+p_m}{q_m} > 1$. Из неравенств (45) видно, что всего комбинаций целочисленных значений p_m и q_m меньше, чем $\sqrt{a}\cdot 2\sqrt{a} = 2a$. Отсюда следует, что меньше чем через $2a$ шагов значения p_m и q_m будут повторяться. Но если $p_{m+\lambda} = p_m$, $q_{m+\lambda} = q_m$, то и $x_{m+\lambda} = x_m$, и $k_{m+\lambda} = k_m$, и $x_{m+\lambda+1} = x_{m+1}$, и $p_{m+\lambda+1} = p_{m+1}$, и $q_{m+\lambda+1} = q_{m+1}$ и т. д. Т. е. наша цепная дробь периодическая.

С другой стороны, мы имеем (по формулам (41)):

$$\frac{\sqrt{a}-p_{m+1}}{q_{m+1}} = \frac{a-p_{m+1}^2}{q_{m+1}(\sqrt{a}+p_{m+1})} = \frac{q_m}{\sqrt{a}+k_m q_m - p_m} = \frac{1}{\frac{\sqrt{a}-p_m}{q_m}+k_m} < 1,$$

ибо

$$\frac{\sqrt{a}-p_m}{q_m} > 0.$$

Далее:

$$\frac{\sqrt{a}-p_m}{q_m} + k_m = \frac{\sqrt{a}+p_{m+1}}{q_m} = \frac{q_{m+1}}{\sqrt{a}-p_{m+1}}$$

по тем же формулам (41). Но мы уже доказали:

$$\frac{\sqrt{a}-p_m}{q_m} < 1;$$

следовательно,

$$k_m = \left[\frac{q_{m+1}}{\sqrt{a}-p_{m+1}}\right]. \qquad (46)$$

Из формулы (46) видно, что при данных q_{m+1} и p_{m+1} k_m однозначно определено, а при данных k_m и x_{m+1} и p_m, и q_m тоже однозначно определены Следовательно, из $p_{m+\lambda} = p_m$, $q_{m+\lambda} = q_m$ вытекает, что и $p_{m+\lambda-1} = p_{m-1}$, $q_{m+\lambda-1} = q_{m-1}$, а далее: $p_{m+\lambda-2} = p_{m-2}$, $q_{m+\lambda-2} = q_{m-2}$, и т. д. Но формула (46) верна только

при $m > 0$; следовательно, для k_0 она уже неверна. Таким образом период нашей цепной дроби начинается с k_1, т. е. со второго звена.

Итак:

Теорема 38. Квадратный корень из целого числа всегда раскладывается в периодическую цепную дробь, период которой начинается со второго звена.

Более глубокие исследования в этой области показывают, что вообще всякая вещественная квадратная иррациональность, т. е. вещественный корень квадратного уравнения с целыми коэффициентами или выражение вида $\frac{b+\sqrt{a}}{c}$, где a, b, c — целые числа, и $a > 0$ раскладывается в периодическую цепную дробь,— чистую или смешанную.

Очень просто доказать обратную теорему.

Теорема 39. Всякая периодическая цепная дробь есть квадратная иррациональность.

Доказательство. Предположим, что данная цепная дробь чисто-периодическая: $x = [(k_1, k_2, \ldots k_m)]$; тогда можно написать:

$$x = k_1 + \cfrac{1}{k_2 + \cdots + \cfrac{1}{k_m + \cfrac{1}{x}}} = (k, k_2, \ldots k_m, x),$$

или: $x = \frac{p_m x + p_{m-1}}{q_m x + q_{m-1}}$; p_m, p_{m-1}, q_m, q_{m-1} — целые положительные числа; следовательно,

$$q_m x^2 + (q_{m-1} - p_m)x - p_{m-1} = 0.$$

Таким образом, x удовлетворяет этому квадратному уравнению (с вещественными корнями).

Предположим теперь, что наша цепная дробь — смешанная периодическая:

$$x = (a_1, a_2, \ldots a_l, (k_1, k_2, \ldots k_m)).$$

Обозначим: $y = ((k_1, k_2, \ldots k_m))$; тогда: $x = (a_1, a_2, \ldots a_l, y)$. Следовательно:

$$x = \frac{p_l y + p_{l-1}}{q_l y + q_{l-1}};$$

y, как значение чисто-периодической дроби, есть квадратная иррациональность; как уже доказано:

$$y = \frac{b + \sqrt{a}}{c}.$$

Подставляя это выражение для y в x, найдем:

$$x = \frac{p_l b + p_{l-1} c + p_l \sqrt{a}}{q_l b + q_{l-1} c + q_l \sqrt{a}}.$$

Уничтожая иррациональность, в знаменателе, найдем для x выражение формы:

$$\frac{B+\sqrt{A}}{C},$$

т. е. и x — квадратная иррациональность.

§ 28. Вернемся к § 23, формуле (32). Пусть мы имеем алгорифм Эвклида для данных чисел r и r_1; r_n — общий наибольший делитель для r и r_1, и формула (32) показывает, что неопределенное уравнение $rx + r_1y = r_n$ всегда имеет целое решение:

$$x = (-1)^{n-1}[k_1, \dots k_{n-1}];\ y = (-1)^n [k_2, \dots k_{n-1}] \qquad (47)$$

Но эти значения x и y не оба положительны. Они имеют разные знаки. В частности, если r и r_1 взаимно-простые, то следующее уравнение имеет целое решение x, y:

$$rx + r_1y = 1.$$

Изменим наше обозначение. Пусть a и b данные целые (не непременно положительные) числа и $D(a, b) = d$. Рассмотрим неопределенное уравнение:

$$ax + by = c, \qquad (48)$$

где c — тоже данное целое число. При любых целых значениях x и y левая часть уравнения (48) делится на d; следовательно, если c не делится на d, то уравнение (48) не имеет целых решений Пусть c делится на d: $c = de$; тогда уравнение $ax + by = d$, как мы видели, имеет целое решение x_1, y_1 (то, что здесь a и b не обязательно положительны, отражается только на комбинации знаков у x_1 и y_1); но тогда x_1e и y_1e представят целое решение уравнения (48). Докажем теперь, что таких целых решений бесчисленное множество. Пусть x_0, y_0 — одно целое решение уравнения (48), а x, y — какое-нибудь иное решение того же уравнения; имеем:

$$ax_0 + by_0 = c;\ ax + by = c;$$

отсюда:

$$a(x - x_0) + b(y - y_0) = 0,$$

или:

$$a(x - x_0) = -b(y - y_0);$$

сократим на d:

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \qquad (49)$$

Левая, а значит, и правая часть формулы (49) делится на $\frac{a}{d}$; но $\frac{b}{d}$ и $\frac{a}{d}$ взаимно-простые, следовательно, $y - y_0$ делится на $\frac{a}{d}$ (по теореме 15 § 7); следовательно, $y - y_0 = \frac{a}{d}t$. Подставляя это значение в формулу (49), найдем: $x - x_0 = -\frac{b}{d}t$.

Итак:

$$\left.\begin{aligned} x &= x_0 - \frac{b}{d}t \\ y &= y_0 + \frac{b}{d}t \end{aligned}\right\} \qquad (50)$$

где t — целое число $\gtrless 0$. Обратно, при любом целом t выражения (50) будут целыми числами, удовлетворяющими уравнению (48), в чем убедимся непосредственно, подставив эти значения для x и y в (48). Таким образом, мы получили следующую основную теорему:

Теорема 40. Неопределенное уравнение (48) имеет целые решения тогда и только тогда, когда его правая часть делится на $d = D(a, b)$ — при этом бесчисленное множество целых решений, которые даются формулами (50). В частности, уравнение $ax + by = d$ имеет решение (47) (с точностью до знаков).

Если $d = 1$, уравнение (48) всегда имеет целые решения; в частности, в этом случае имеет целые решения и уравнение:

$$ax + by = 1. \qquad (51)$$

Практически мы найдем решение (47), применяя к числам a и b алгорифм Эвклида или разлагая $\frac{|a|}{|b|}$ (пусть $|a| > |b|$) в цепную дробь и беря за $|x|$ и $|y|$ — знаменатель и числитель предпоследней подходящей дроби $\frac{[k_1, \ldots k_{n-1}]}{[k_2, \ldots k_{n-1}]}$. При $|a| > |b|$ должно быть $|x| < |y|$; знаки же у x и y берутся так, чтобы ax и by имели разные знаки и чтобы было: $\big||ax| - |by|\big| = 1$ Вычисляя последние цифры в произведениях $|ax|$ и $|by|$, легко сообразить, какие должны быть знаки у x и y.

Пример 1. Найти целые решения уравнения:

$$15x + 19y = 1.$$

Применив алгорифм Эвклида, найдем:

$$\begin{aligned} 19 : 15 &= 1 \\ 15 : 4 &= 3 \\ 4 : 3 &= 1 \\ 3 : 1 &= 3 \end{aligned}$$

Последнее частное (3) отбрасываем, ибо оно $= k_n$, а в формулы (47) k_n не входит. Все остальные частные пишем в обратном порядке:

$k_{n-1}, k_{n-2}, \ldots k_1$, применяя формулу (28)

$$\frac{1 \quad 3 \quad 1}{1 \quad 1 \quad 4 \quad 5}.$$

Следовательно, $|x| = 5$, $|y| = 4$ (ибо здесь x с меньшим коэффициентом). Для определения знаков у x и y вычисляем послед-

ние цифры произведений $15 \cdot 5$ и $19 \cdot 4$; они здесь 5 и 6. Но $6 - 5 = 1$, следовательно, $x = -5$, $y = +4$. Общее решение есть:

$$x = -5 \pm 19t; \quad y = 4 \mp 15t.$$

(Мы написали двойной знак у t, ибо всегда можно написать $-t$ вместо t).

Пример 2. Найти целые решения уравнения:

$$126x - 102y = 18.$$

Здесь $D(126, 102) = 6$, но 18 делится на 6; сократив на 6, получим:

$$21x - 17y = 3.$$

Решим сначала уравнение:

$$21x - 17y = 1.$$

Имеем:

$$\begin{array}{r} 21 : 17 = 1 \\ 17 : 4 = 4 \\ 4 : 1 = 4 \end{array} \qquad \begin{array}{ccc} & 4 & 1 \\ \hline 1 & 4 & 5 \end{array}$$

Следовательно, $|x| = 4$, $|y| = 5$. Вычисляем последние цифры произведений $21 \cdot 4$; $17 \cdot 5$; они 4 и 5; но $-21 \cdot 4 + 17 \cdot 5 = 1$. Значит, должно быть:

$$x = -4, \; y = -5.$$

Для уравнения: $21x - 17y = 3$:

$$x = -4 \cdot 3 = -12, \; y = -5 \cdot 3 = -15.$$

Общее решение данного уравнения:

$$x = -12 \pm 17t; \; y = -15 \pm 21t.$$

(Здесь мы оба раза пишем $\pm$, так как коэффициенты нашего уравнения имеют разные знаки). Беря знак $+$ и $t = 1$, получим положительное решение: $x = 5$, $y = 6$.

§ 29. Обобщим теперь теорему 40 на случай нескольких неизвестных. Пусть $a_1, a_2, \dots a_m$ — данные целые числа и $D(a_1, a_2, \dots a_m) = d$; пусть уже доказано, что уравнение

$$a_1x_1 + a_2x_2 + \dots + a_mx_m = d \tag{52}$$

имеет целое решение $x_1, x_2, \dots x_m$. Пусть нам дано еще одно целое число a_{m+1}. Докажем, что тогда и уравнение

$$a_1u_1 + a_2u_2 + \dots + a_mu_m + a_{m+1}u_{m+1} = \delta, \tag{53}$$

где $\delta = D(a_1, a_2, \dots a_m, a_{m+1})$, тоже имеет целое решение $u_1, u_2, \dots u_m, u_{m+1}$.

По теореме 13, § 6, $\delta = D(d, a_{m+1})$, следовательно, по теореме 40 уравнение $dy + a_{m+1}u_{m+1} = \delta$ имеет целое решение y, a_{m+1}. Подставляя сюда вместо d его выражение $a_1x_1 + a_2x_2 + \dots + a_mx_m$

из (52) и обозначая $u_1 = x_1y$, $u_2 = x_2y$, ... $u_m = x_my$, найдем целое решение уравнения (53). Этим доказано, что уравнение (52) имеет целое решение при всяком m.

Далее, как и в случае двух неизвестных, непосредственно выводится, что общее уравнение

$$a_1x_1 + a_2x_2 + \ldots + a_mx_m = c \tag{54}$$

имеет целое решение тогда и только тогда, когда c делится на d.

Обозначим в этом случае: $c = dx$; тогда по (54) имеем:

$$a_1x_1 + a_2x_2 + \ldots + a_mx_m = dx. \tag{55}$$

Всякой системе целых чисел $x_1, x_2, \ldots x_m$ соответствует определенное целое число x. Но и обратно: каждому целому x соответствует система (даже бесчисленное множество таких систем) целых значений $x_1, x_2, \ldots x_m$, удовлетворяющая уравнению (55). Иными словами: всякое целое число, представляемое в форме $a_1x_1 + a_2x_2 + \ldots + a_mx_m$ (при целых $x_1, x_2, \ldots x_m$), представимо и в форме dx (при целом x); и обратно. Это выражают, говоря, что обе эти формы эквивалентны.

Итак:

Теорема 41. Линейная однородная форма (с целыми коэффициентами) от какого угодно числа переменных всегда эквивалентна линейной однородной форме от одного переменного (тоже с целым коэффициентом).

Эта теорема весьма важна.

Покажем на примерах, как найти целые решения неопределенного линейного уравнения с несколькими неизвестными.

Пример 3. Дано уравнение:

$$25x - 13y + 7z = 4.$$

Делим все коэффициенты левой части на наименьший из них, т. е. на 7, и берем неполные (или полные, если деление окажется без остатка) частные. Обозначим:

$$3x - y + z = u; \tag{I}$$

умножаем это снова на 7 и вычитаем из данного уравнения:

$$4x - 6y = 4 - 7u,$$

или:

$$4x - 6y + 7u = 4.$$

Но это уравнение с неизвестными x, y, u того же типа, что́ и данное, только наибольший коэффициент здесь $= 7$, тот же, что в данном уравнении, — наименьший. Делим здесь левую часть на 4 и обозначаем:

$$x - y + u = v; \tag{II}$$

умножаем на 4 и отнимаем:

$$-2y + 3u = 4 - 4v,$$

или:

$$-2y + 3u + 4v = 4.$$

Делим здесь левую часть на 2 и обозначаем:

$$-y + u + 2v = w; \qquad \text{(III)}$$

умножаем на 2 и отнимаем:

$$u = 4 - 2w.$$

Подставляя это значение для u в (III), находим:

$$-y + 4 - 2w + 2v = w,$$

или:

$$y = 4 + 2v - 3w. \qquad \text{(IV)}$$

Подставляя значения для u и y во (II), находим:

$$x - 4 - 2v + 3w + 4 - 2w = v,$$

или:

$$x = 3v - w. \qquad \text{(V)}$$

Наконец, подставляя в (I) значения для x, y, u, находим:

$$9v - 3w - 4 - 2v + 3w + z = 4 - 2w,$$

или:

$$z = 8 - 7v - 2w. \qquad \text{(VI)}$$

Очевидно, что при произвольных целых значениях v и w и x, y, z будут целые. Таким образом (IV), (V), (VI) и дают общее целое решение нашего уравнения; оно зависит от двух целых параметров v и w.

Этот способ можно применить и к уравнениям с двумя неизвестными.

Пример 4. Дано уравнение:

$$7x_1 + 4x_2 - 2x_3 + 3x_4 = 2. \qquad \text{(I)}$$

Делим все коэффициенты левой части на наименьший из них (по абсолютной величине) и берем неполные (или полные, когда деление без остатка) частные; обозначим:

$$3x_1 + 2x_2 - x_3 + x_4 = u. \qquad \text{(II)}$$

Обе части этого равенства множим на 2 (т. е. на тот коэффициент, на который мы делили) и результат отнимаем от данного уравнения (I). Получим:

$$x_1 + x_4 = 2 - 2u;$$

отсюда:

$$x_1 = 2 - 2u - x_4. \qquad \text{(III)}$$

Подставляя это выражение для x_1 в (II), найдем:

$$6 - 6u - 3x_4 + 2x_2 - x_3 + x_4 = u,$$

или:

$$x_3 = 6 - 7u - 2x_4 + 2x_2. \qquad \text{(IV)}$$

Мы видим из (III) и (IV), что, давая для u, x_4, x_1 произвольные целые значения, мы получим и для x_1 и x_3 целые значения. Таким образом, формулы

$$x_1 = 2 - 2u - v,\ x_2 = w,\ x_3 = 6 - 7u - 2v + 2w,\ x_4 = v$$

и дают нам общее целое решение уравнения (I). Оно зависит от трех целых параметров u, v, w (случайно здесь два из этих параметров — наши неизвестные x_2 и x_4). При $u = v = w = 0$ имеем частное решение:

$$x_1 = 2,\ x_2 = 0,\ x_3 = 6,\ x_4 = 0.$$

§ 30. Теорема 40, особенно та ее часть, где говорится о существовании целых решений уравнения $ax + by = d = D(a, b)$, является основной в теории делимости целых чисел. Она непосредственно вытекает из алгорифма Эвклида, который сам основан на теореме 1 о делении с остатком двух целых чисел.

Основываясь на теореме 40, можно построить всю теорию делимости целых чисел,— вывести все теоремы о делимости, которые мы имели в главе I. Например, пусть a и c взаимно-простые; тогда по теореме 40 существуют такие целые числа x, y, что $ax + cy = 1$. Умножим это на b:

$$abx + cby = b. \qquad (56)$$

Пусть ab делится на c; тогда из (56) видно, что вся левая часть, а значит и правая, т. е. b, делится на c; это — теорема 15, которую мы, таким образом, еще раз доказали. Далее, из (56) ясно, что всякий общий делитель ab и c является также делителем для b, а следовательно, $D(ab, c) = D(b, c)$; это — теорема 16. Из теоремы 15 непосредственно вытекает теорема 19, а на этой теореме основана теорема об однозначности разложения числа на простые множители (у нас — теорема 21).

§ 31. Применим теорию цепных дробей к доказательству одной важной теоремы о простых числах вида $4s + 1$. Пусть p такое простое число. Рассмотрим дроби $\frac{p}{2}$, $\frac{p}{3}$, ... $\frac{p}{2s}$; все они > 2 и несократимы. Разложим каждую из них в цепную дробь. Пусть q — одно из чисел 2, 3, ... $2s$ и пусть:

$$\frac{p}{q} = k_1 + \cfrac{1}{k_2 + \cdots + \cfrac{1}{k_n}} = \frac{[k_1, k_2, \ldots k_n]}{[k_2, \ldots k_n]}. \qquad (57)$$

Здесь $k_1 \geqq 2$, $k_n > 1$, $n > 1$, ибо $\frac{p}{q}$ — не целое число. По формуле (33) § 23 дробь в правой части (57) несократимая; следовательно:

$$p = [k_1, k_2, \ldots k_n];\ q = [k_2, \ldots k_n].$$

Обратно, если мы нашли каким-нибудь способом представление p скобками Эйлера

$$p = [k_1, k_2, \ldots k_n],$$

где $k_1 > 1$, $k_n > 1$, $n > 1$, то, написав $\frac{p}{q} = k_1 + \cfrac{1}{k_2 + \cdots + \cfrac{1}{k_n}}$,

мы будем иметь: $q = [k_2, \ldots k_n] < \frac{p}{2}$, ибо $\frac{p}{q} > 2$, т. е. q — одно из чисел 2, 3, ... $2s$. Но по формуле (28) § 23 также

$$p = [k_n, k_{n-1}, \ldots k_1];$$

следовательно, если обозначим: $\frac{p}{q'} = k_n + \cfrac{1}{k_{n-1} + \cdots + \cfrac{1}{k_1}}$, то $q' = [k_{n-1}, \ldots k_1]$ — тоже одно из чисел 2, 3, ... $2s$.

Таким образом, эти числа распределяются по парам — таких чисел, как q и q'; но всего этих чисел $2s - 1$ — нечетное число. Следовательно, непременно встретится и такой случай, когда $q' = q$, т. е. $k_n = k_1$, $k_{n-1} = k_2$, ...

Рассмотрим этот случай. Пусть $n = 2m + 1$ — нечетное число; тогда:

$$p = [k_1, k_2, \ldots k_{m-1}, k_m, k_{m+1}, k_m, k_{m-1}, \ldots k_1];$$

или, применяя формулы (29) и (28) § 23:

$$p = [k_1, \ldots k_m] [k_{m+1}, k_m, \ldots k_1] + [k_1, \ldots k_{m-1}] [k_m, \ldots k_1] = \\ = [k_1, \ldots k_m] \cdot \{ [k_1, \ldots k_{m+1}] + [k_1, \ldots k_{m-1}] \}.$$

Но это значит, что p разложено на два целых множителя и каждый из них > 1; этого не может быть, ибо p — простое число. Следовательно, $n = 2m$ — четное, и мы получим по тем же формулам (29), (28) § 23:

$$p = [k_1, \ldots k_m, k_m, \ldots k_1] = [k_1, \ldots k_m] [k_m, \ldots k_1] + \\ + [k_1, \ldots k_{m-1}] [k_{m-1}, \ldots k_1] = [k_1, \ldots k_m]^2 + [k_1, \ldots k_{m-1}]^2.$$

Т. е. мы доказали следующее:

Теорема 42. Всякое простое число вида $4s + 1$ может быть представлено как сумма двух квадратов *).

Пример. Пусть $p = 73$; при $q = 27$ имеем:

$$\frac{73}{27} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2}}}}}.$$

Здесь $n = 6$, $k_1 = k_6 = 2$, $k_2 = k_5 = 1$, $k_3 = k_4 = 2$; следовательно: $73 = [2, 1, 2]^2 + [2, 1]^2 = 8^2 + 3^2$.

---

*) В дальнейшем (в гл. VI, § 71) мы докажем, что это представление однозначно.

УПРАЖНЕНИЯ.

22. Посредством алгорифма Эвклида найти: а) $D(549, 387)$; б) $D(589, 343)$; в) $D(12606, 6494)$ (§ 19).

Ответ. а) 9; б) 1; в) 382.

23. Разложить в цепные дроби следующие обыкновенные дроби: а) $\frac{95122}{53808}$; б) 2,3547; в) $\frac{99}{170}$ (§ 20).

Ответ. а) (1, 1, 3, 3, 3, 1, 5, 4, 4, 1, 3);
б) (2, 2, 1, 4, 1, 1, 6, 1, 20, 2);
в) (0, 1, 1, 2, 1, 1, 6, 2).

24. Разложить в периодические цепные дроби и вычислить с точностью до 0,0001: а) $\sqrt{5}$; б) $\sqrt{13}$; в) $\sqrt{42}$; г) $\sqrt{59}$ (§ 21, 24, 25).

Ответ. а) $(2, (4)) \approx 2{,}2361$; б) $(3, (1, 1, 1, 1, 6)) \approx 3{,}6056$;
в) $(6, (2, 12)) \approx 6{,}4807$; г) $(7, (1, 2, 7, 2, 1, 14)) \approx$
$\approx 7{,}6812$.

25. При помощи цепных дробей вычислить с точностью до 0,0001 оба корня уравнения $3x^2 - 7x - 3 = 0$ (§ 21, 24, 25).

Ответ. $x_1 = ((2, 1, 2)) \approx 2{,}7032$; $x_2 = (-1, 1, 1, (1, 2, 2)) \approx$ $\approx -0{,}3699$.

26. При помощи цепных дробей вычислить оба корня уравнения $x^2 + 9x + 6 = 0$ с точностью до 0,0001 (§ 21, 24, 25).

Ответ. $x_1 = (-1, 3, (1, 1, 1, 3, 7, 3)) \approx -0{,}7250$;
$x_2 = (-9, 1, 2, (1, 1, 1, 3, 7, 3)) \approx -8{,}2750$.

27. При помощи цепных дробей вычислить все корни уравнения $x^3 - x^2 - 2x + 1 = 0$ с точностью до 0,0001 (§ 21, 24, 25).

Ответ. $x_1 = (1, 1, 4, 20, \ldots) \approx 1{,}8019$;
$x_2 = (0, 2, 4, 20, \ldots) \approx 0{,}4450$;
$x_3 = (-2, 1, 3, 20, 2, \ldots) \approx -1{,}2469$.

28. Вычислить скобки Эйлера: а) $[1, 0, 2, 0, 3]$; б) $\left[1, \frac{1}{2}, \frac{1}{2}, 2\right]$; в) $[2, -2, 3, -3, 1, -4]$; г) $[\alpha, \beta, \gamma, \delta]$; д) $\left[3, 0, \frac{1}{2}, 0, 0, 1\right]$ (§ 22).

Ответ. а) 6; б) 5; в) −26; г) $\alpha\beta\gamma\delta + \alpha\beta + \gamma\delta + \alpha\delta + 1$; д) $4\frac{1}{2}$.

29. Проверить на примере $[1, 2, 1, 3, 2, 3, 2]$ формулу (29) § 23 при $m = 3$ (§ 23).

30. Найти первые пять подходящих дробей разложения в цепную дробь числа $\pi = 3{,}1415926535897\ldots$ (§ 24, 25).

Ответ. $\frac{3}{1}$; $\frac{22}{7}$; $\frac{333}{106}$; $\frac{355}{113}$; $\frac{103993}{33102}$.

31. Найти первые пять подходящих дробей разложения в цепную дробь числа $e = 2{,}71828182845904\ldots$ (§ 24, 25).

Ответ. 2, 3, $\frac{8}{3}$, $\frac{11}{4}$, $\frac{19}{7}$.

32. В каких уравнениях корни разлагаются в следующие цепные дроби: а) ((2, 4, 1, 3)); б) ((1, 2, 4, 6)); в) (2, 1, 2, (1, 1, 3)); г) (4, (1, 1, 2, 1, 1, 8))? (§ 27).

Ответ. а) $19x^2 - 37x - 11 = 0$; б) $56x^2 - 72x - 13 = 0$; в) $2x^2 - 15x + 26 = 0$; г) $x^2 - 21 = 0$.

33. Найти все целые решения уравнения $253x - 449y = 1$ (§ 28).

Ответ. $x = -126 + 449t$; $y = -71 + 253t$.

34. Найти целые решения уравнения $53x + 47y = 11$ (§ 28).

Ответ. $x = -6 + 47t$; $y = 7 - 53t$.

35. Найти целые решения уравнения $[\alpha, \beta, \gamma, \delta]\, x - [\beta, \gamma, \delta]\, y = 1$, где α, β, γ, δ — целые числа (§ 28).

Ответ. $x = [\beta, \gamma] + [\beta, \gamma, \delta]\, t$; $y = [\alpha, \beta, \gamma] + [\alpha, \beta, \gamma, \delta]\, t$.

36. Найти целые решения уравнений: а) $24x + 56y = 64$; б) $81x - 48y = 33$; в) $22x + 32y = 48$; г) $36x - 15y = 8$ (§ 28).

Ответ: а) $x = -2 + 7t$, $y = 2 - 3t$; б) $x = 1 + 16t$, $y = 1 + 27t$; в) $x = -8 + 16t$, $y = 7 - 11t$; г) целых решений нет.

37. Найти целые решения уравнения $6x - 5y + 3z = 1$ (§ 29).

Ответ. $x = u$, $y = 1 - 3v$, $z = 2 - 2u - 5v$.

38. Найти целые решения уравнения $5x_1 + 4x_2 - 7x_3 - 3x_4 = 5$ (§ 29).

Ответ. $x_1 = u$, $x_2 = 5 - 2u - 3v + w$, $x_3 = w$, $x_4 = 5 - u - 4v - w$.

39. Способом § 31 представить число 61 как сумму двух квадратов (§ 31).

Ответ. $\frac{61}{11} = (5, 1, 1, 5)$; $61 = 5^2 + 6^2$.

40. То же самое для числа 137 (§ 31).

Ответ. $\frac{137}{37} = (3, 1, 2, 2, 1, 3)$; $137 = 4^2 + 11^2$.

ГЛАВА III

СРАВНЕНИЯ

§ 32. Пусть m — данное целое положительное число; вместе с ним рассмотрим и все его кратные km, где k — любое целое число $\gtreqless 0$ или $= 0$. Система всех этих кратных есть так называемый «модуль» *). Если разность двух целых чисел a и b делится на m или *принадлежит к модулю* m, то такие числа называются *сравнимыми по модулю* m. Это обозначается таким символом:

$$a \equiv b \pmod{m}. \tag{58}$$

Некоторые авторы обозначают короче:

$$a \equiv b\ (m).$$

Такое соотношение между числами a и b называется *сравнением* или *конгруенцией*. Из него видно, что числа a и b при делении на m дают одинаковые остатки.

Теорема 43. Для сравнений выполнены три основных закона равенств: симметрии, транзитивности и рефлексивности.

Разъяснение. Закон симметрии говорит, что при $a = b$ и $b = a$; закон транзитивности: из $a = b$, $b = c$ следует $a = c$; закон рефлексивности: $a = a$.

Если для некоторого соотношения выполнены эти три закона, то говорят, что это соотношение имеет *характер равенства*. Таким образом, теорема 43 говорит, что сравнение имеет характер равенства.

---

*) Вообще модулем называется система M чисел, имеющая следующее свойство: если a и b принадлежат к M, то и $a \pm b$ тоже принадлежат к M (иными словами: *M — группа относительно сложения*). Легко доказать, что в области целых рациональных чисел всякий модуль есть система кратных некоторого целого числа $m > 0$. Действительно, пусть m — наименьшее положительное число данного модуля M, а n — какое-нибудь другое число из M. Делим n на m и обозначаем через q — частное, через r — остаток этого деления. Имеем: $0 \leqq r < m$; $n - qm = r$. Отсюда видно, что r тоже принадлежит к M, следовательно, $r = 0$ (ибо m — *наименьшее* положительное число из M), т. е. $n = mq$.

Доказательство. 1) Если $a-b$ делится на m, то и $b-a$ тоже делится на m; таким образом, из $a \equiv b$ *) следует $b \equiv a \pmod{m}$.

2) Если $a-b$ и $b-c$ делятся на m, то $(a-b)+(b-c)=$ $=a-c$ тоже делится на m; т. е. из $a \equiv b$, $b \equiv c$ следует $a \equiv c \pmod{m}$.

3) $a-a=0$ делится на всякое целое число m; следовательно, $a \equiv a \pmod{m}$.

Замечание. Формула $a \equiv 0 \pmod{m}$ говорит, что число a делится на m; формула $a \equiv b \pmod{m}$ равнозначна с формулой $a-b \equiv 0 \pmod{m}$.

Всякое (целое) число сравнимо по модулю m со своим остатком от деления этого числа на m. Но от деления на m могут получиться только следующие остатки: или 0, или 1, или 2, ... или $m-1$. Никакие два из этих остатков не сравнимы друг с другом по модулю m. Иными словами, все целые числа распределяются по m классам; первый класс составляют все числа, которые делятся на m (т. е. этот класс и составляет самый модуль m); второй класс составляют все числа, которые при делении на m дают остаток 1, и т. д.; последний класс (m-й) состоит из чисел, дающих при делении на m остаток $m-1$.

Итак:

Теорема 44. Все целые числа распределяются относительно данного модуля m на m классов так, что все числа одного и того же класса сравнимы друг с другом по модулю m, тогда как числа разных классов не сравнимы друг с другом по модулю m.

Заметим, что такое распределение чисел на классы относительно данного соотношения возможно тогда и только тогда, когда для этого соотношения выполнены три основных закона теоремы 43.

Если из каждого из m классов, на которые распадаются все целые числа по модулю m, взять по одному числу, то эти m взятых чисел составляют *полную систему вычетов* по модулю m. Полная система вычетов имеет два характерных свойства, а именно:

I. Никакие два числа из полной системы вычетов по модулю m не сравнимы друг с другом по модулю m.

II. Всякое целое число непременно сравнимо по модулю m с одним (и только с одним) числом из полной системы вычетов по модулю m.

Каждое из этих двух свойств вполне определяет данную систему m чисел, как полную систему вычетов по модулю m.

Примеры полной системы вычетов по модулю m:

1) 0, 1, 2, 3, ... $m-1$; это — так называемые *наименьшие положительные вычеты* (остатки от деления чисел на m);

---

*) Если рассматривают несколько сравнений по одному и тому же модулю m, то обозначение $(\bmod m)$ часто пропускают.

2) 0, —1, —2, —3, ... —$(m-1)$; это *наименьшие отрицательные вычеты;*

3) 0, ± 1, ± 2, ... $\pm\frac{m-1}{2}$, если m нечетное;

$$0,\ \pm 1,\ \pm 2,\ \ldots \pm\left(\frac{m}{2}-1\right),\ +\frac{m}{2}\ \left(\text{или } -\frac{m}{2} \text{ вместо } +\frac{m}{2}\right),$$

если m — четное; это — *абсолютно-наименьшие вычеты.*

4) Если a — какое-нибудь целое число, то числа a, $a+1$, $a+2$, ... $a+m-1$ образуют полную систему вычетов по модулю m, ибо свойство I для нее выполнено.

5) Если a — *взаимно-простое* с m, то числа 0, a, $2a$, ... $(m-1)a$ (вместо 0 можно взять ma) образуют полную систему вычетов по модулю m, ибо свойство I здесь выполнено: если $\varkappa a\equiv\lambda a\ (\mathrm{mod}\, m)$, то, следовательно, $\varkappa a-\lambda a=(\varkappa-\lambda)a$ делится на m; но $D(a, m) = 1$, значит (по теореме 15, § 7) $\varkappa-\lambda$ делится на m; но $|\varkappa-\lambda| < m$, следовательно, при $\varkappa\neq\lambda$ этого не может быть.

Таким образом, в зависимости от модуля m всякое целое число непременно представляется одною из форм: km, $km+1$, $km+2$, ... $km+m-1$, или: km, $km-1$, $km-2$, ... $km-m+1$. Например, при $m=2$ имеем две такие формы: $2k$, $2k+1$ (или $2k-1$). Первая — форма *четных* чисел, вторая — форма *нечетных* чисел. При $m=3$ имеем три формы: $3k$, $3k+1$, $3k+2$ (или $3k-1$). При $m=4$ имеем четыре формы: $4k$, $4k+1$, $4k+2$, $4k+3$ (или $4k-1$). И т. д.

§ 33. Основные свойства сравнений. Эти свойства являются просто следствиями соответствующих теорем о делимости (глава I).

Теорема 45. Если $a\equiv b\ (\mathrm{mod}\, m)$ и m делится на k, то и $a\equiv b\ (\mathrm{mod}\, k)$. Это следует непосредственно из теоремы 2, § 2.

Теорема 46. Если $a\equiv b\ (\mathrm{mod}\, k_1)$, $a\equiv b\ (\mathrm{mod}\, k_2)$, ... $a\equiv b\ (\mathrm{mod}\, k_n)$ и $M(k_1, k_2, \ldots k_n)=m$, то $a\equiv b\ (\mathrm{mod}\, m)$.

Это вытекает из теоремы 8, § 3, ибо $a-b$ — общее кратное для k_1, k_2, ... k_n.

Теорема 47. Если $a\equiv b\ (\mathrm{mod}\, m)$, то $ac\equiv bc\ (\mathrm{mod}\, |mc|)$.

Действительно:

$$\frac{ac-bc}{mc}=\frac{a-b}{m}.$$

Следствие. Если $a\equiv b\ (\mathrm{mod}\, m)$, то $ac\equiv bc\ (\mathrm{mod}\, m)$.

Это вытекает из теорем 47 и 45.

Теорема 48. Сравнения с одним и тем же модулем можно почленно складывать.

Доказательство. Пусть $a\equiv b\ (\mathrm{mod}\, m)$, $a_1\equiv b_1\ (\mathrm{mod}\, m)$, т. е. $a-b$ и a_1-b_1 делятся на m. Но тогда и их сумма $(a-b)+(a_1-b_1)=(a+a_1)-(b+b_1)$ делится на m, следовательно $a+a_1\equiv b+b_1\ (\mathrm{mod}\, m)$.

Это непосредственно обобщается и на несколько сравнений.

Следствие 1. Сравнение с одним и тем же модулем можно почленно вычитать.

Действительно: из $a_1 \equiv b_1 \pmod{m}$ следует: $-a_1 \equiv -b_1 \pmod{m}$ (см. следствие из теоремы 47 при $c = -1$); следовательно, $a - a_1 \equiv b - b_1 \pmod{m}$.

Следствие 2. Можно прибавить к обеим частям или отнять от обеих частей сравнения одно и то же число: если $a \equiv b \pmod{m}$, то $a \pm c \equiv b \pm c \pmod{m}$, так как $c \equiv c$.

Отсюда непосредственно выводим:

Следствие 3. В сравнениях, как и в равенствах, можно переносить члены из одной части в другую с противоположными знаками.

Теорема 49. Сравнения с одним и тем же модулем можно почленно перемножать.

Доказательство. Пусть $a \equiv b \pmod{m}$, $a_1 \equiv b_1 \pmod{m}$; тогда (по следствию из теоремы 47) $aa_1 \equiv ba_1$, $ba_1 \equiv bb_1 \pmod{m}$. Отсюда (по закону транзитивности) $aa_1 \equiv bb_1 \pmod{m}$.

Это непосредственно обобщается на несколько сравнений.

Следствие. Обе части сравнения можно возвысить в степень с одним и тем же натуральным показателем.

Теорема 50. Если $ac \equiv bc \pmod{m}$ и $D(c, m) = d$, то $a \equiv b \left(\operatorname{mod} \frac{m}{d}\right)$.

Доказательство. Пусть $c = c_1 d$, $m = m_1 d$; тогда: $\frac{ac - bc}{m} = \frac{(a-b)c}{m} = \frac{(a-b)c_1}{m_1}$. Это — целое число, т. е. $(a - b)c_1$ делится на m_1; но c_1 и m_1 — взаимно-простые (по теореме 10, § 4), следовательно (по теореме 15, § 7), $a - b$ делится на m_1, т. е. $a \equiv b \pmod{m_1}$.

Важны следующие два предельных случая этой теоремы.

Следствие 1. Если $d = c$, т. е. m делится на c, то из $ac \equiv bc \pmod{m}$ следует: $a \equiv b \left(\operatorname{mod} \frac{m}{c}\right)$. Иными словами: обе части сравнения и модуль можно сократить на их общий множитель.

Следствие 2. Если $d = 1$, т. е. m и c взаимно-простые, то из $ac \equiv bc \pmod{m}$ следует: $a \equiv b \pmod{m}$. Иными словами: обе части сравнения можно сократить на их общий множитель, если только он взаимно-простой с модулем. Например: $24 \equiv 4 \pmod{10}$, но $6 \not\equiv 1 \pmod{10}$.

Замечание. Таким образом, в области действий умножения и деления нет полной аналогии сравнений с равенствами.

Из предыдущих теорем и следствий вытекает следующая общая теорема:

Теорема 51. Пусть $f(a, b, c, \ldots)$ — произвольная целая рациональная функция от целых чисел $a, b, c, \ldots$ (постоянных или переменных, известных или неизвестных) с целыми коэффициентами. Если $a \equiv a_1$, $b \equiv b_1$. $c \equiv c_1, \ldots \pmod{m}$, то и

$$f(a, b, c, \ldots) \equiv f(a_1, b_1, c_1, \ldots) \pmod{m}.$$

Иначе: сравнение не нарушится, если числа, входящие в какую-нибудь его часть, заменить какими-небудь сравнимыми с ними числами по тому же самому модулю. (Очевидно, что обе части сравнения только и могут быть целыми рациональными функциями от целых чисел).

Доказательство. Пусть $f(a, b, c, \ldots) = \sum Ca^\alpha b^\beta c^\gamma \ldots$, где C — какие-нибудь целые коэффициенты. Имеем по следствию из теоремы 49:

$$a^\alpha \equiv a_1^\alpha,\ b^\beta \equiv b_1^\beta,\ c^\gamma \equiv c_1^\gamma, \ldots,$$

а по самой теореме 49 и по следствию из теоремы 47:

$$Ca^\alpha b^\beta c^\gamma \ldots \equiv Ca_1^\alpha b_1^\beta c_1^\gamma \ldots;$$

наконец, по теореме 48:

$$\sum Ca^\alpha b^\beta c^\gamma \ldots \equiv \sum Ca_1^\alpha b_1^\beta c_1^\gamma \ldots$$

и теорема 51 доказана.

Доказанная теорема позволяет заменить в сравнении все постоянные известные коэффициенты их наименьшими вычетами,— положительными, или абсолютно-наименьшими по данному модулю. В частности, все числа, делящиеся на модуль, можно заменить нулями. Можно при желании все коэффициенты в сравнении сделать положительными.

Заметим, что теоремы 48 и 49 определяют действия сложения и умножения над классами по данному модулю m, ибо если число a принадлежит к классу A, а число b принадлежит к классу B, то $A + B$ можно определить как класс, к которому принадлежит $a + b$. По теореме 48 этот класс определяется однозначно, т. е. независимо от выбора представителей a, b его слагаемых A и B. Подобно же, класс AB определяется как класс, к которому принадлежит число ab; по теореме 49 он тоже определяется однозначно.

§ 34. Некоторые частные случаи. Теорема 52. Квадрат всякого нечетного числа сравним с единицей по модулю 8.

Доказательство. Всякое нечетное число имеет вид: $4k \pm 1$. Беря сравнение по модулю 8, имеем:

$$(4k \pm 1)^2 = 16k^2 \pm 8k + 1 \equiv 1 \pmod 8,$$

и наша теорема доказана.

Теорема 53. Нечетное число вида $4k + 3$ нельзя представить как сумму двух квадратов (целых чисел).

Доказательство. Пусть x и y — любые целые числа. Если они оба четные или оба нечетные, то $x^2 + y^2$ — четное. Если же, например, x — четное, а y — нечетное, то x^2 делится на 4, т. е. $x^2 \equiv 0 \pmod 4$, а по теореме 52 $y^2 \equiv 1 \pmod 8$, т. е. и $y^2 \equiv 1 \pmod 4$. Следовательно (по теореме 48):

$$x^2 + y^2 \equiv 1 \pmod 4.$$

Таким образом, никогда не бывает, чтобы x^2+y^2 было $\equiv 3 \pmod 4$, чем и доказана наша теорема.

Замечание. Теорема 53 применима для всех чисел формы $4k+3$, в частности, и для простых чисел такой формы. Таким образом, она является дополнением к теореме 42, относящейся к простым числам формы $4k+1$ (но только к *простым* числам такой формы).

§ 35. Функция $\varphi(m)$ *). Через $\varphi(m)$ обозначается число (целых положительных) чисел, меньших данного (целого положительного) числа m и взаимно-простых с m. Кроме того, дополнительно определяется $\varphi(1)=1$. Эту функцию $\varphi(m)$ можно еще определить так: она есть число классов чисел по модулю m взаимно-простых с m, или — число чисел, взаимно-простых с m, из какой-нибудь полной системы вычетов по модулю m **).

Выведем формулу для вычисления функции $\varphi(m)$.

Если $m=p$ — простое число, то очевидно, что все целые числа >0 и $<p$ — взаимно-простые с p; следовательно,

$$\varphi(p)=p-1. \tag{59}$$

Если $m=p^\alpha$ — степень простого числа, то из чисел >0 и $<p^\alpha$ делятся на p только следующие: $p, 2p, 3p, \ldots (p^{\alpha-1}-1)p$; их число: $p^{\alpha-1}-1$. Все остальные числа >0 и $<p^\alpha$ не делятся на p, следовательно, — взаимно-простые с p^α. Таким образом:

$$\varphi(p^\alpha)=(p^\alpha-1)-(p^{\alpha-1}-1)=p^\alpha-p^{\alpha-1}=p^{\alpha-1}(p-1)=p^\alpha\left(1-\frac{1}{p}\right). \tag{60}$$

Для дальнейшего необходима следующая вспомогательная теорема:

Теорема 54. Если переменная x пробегает полную систему вычетов по модулю a, а переменная y пробегает полную систему вычетов по модулю b и a и b взаимно-простые, то $z=ay+bx$ пробегает полную систему вычетов по модулю ab; z тогда и только тогда взаимно-простое с ab, когда x взаимно-простое с a, а y взаимно-простое с b.

Доказательство. x принимает a значений, y принимает b значений; комбинируя каждое значение x с каждым значением y, получим ab значений для z. Докажем, что никакие два из этих значений z не сравнимы по модулю ab. Пусть

$$z_1=ay_1+bx_1, \quad z_2=ay_2+bx_2$$

и пусть

$$ay_1+bx_1 \equiv ay_2+bx_2 \pmod{ab};$$

тогда (по теореме 45): $ay_1+bx_1 \equiv ay_2+bx_2 \pmod a$; $ay_1+bx_1 \equiv$ $\equiv ay_2+bx_2 \pmod b$.

*) Эту функцию ввел и исследовал Эйлер.

**) Легко видеть, что все числа данного класса по модулю m имеют один и тот же общий наибольший делитель с m.

Отсюда (по теореме 51):

$$bx_1 \equiv bx_2 \pmod{a}; \quad ay_1 \equiv ay_2 \pmod{b}$$

и по следствию 2 из теоремы 50:

$$x_1 \equiv x_2 \pmod{a}; \quad y_1 \equiv y_2 \pmod{b}.$$

Но x_1 и x_2 числа из полной системы вычетов по модулю a; если они различны, то они несравнимы по модулю a, следовательно, $x_1 = x_2$. Аналогично найдем: $y_1 = y_2$, т. е. $z_1 = z_2$. Этим доказана первая часть нашей теоремы.

Пусть $z = ay + bx$ взаимно-простое с ab, а следовательно, и с a и с b отдельно; тогда $z - ay = bx$ взаимно-простое с a, т. е. и x взаимно-простое с a. Аналогично, $z - bx = ay$ взаимно-простое с b, т. е. и y взаимно-простое с b.

Пусть теперь, обратно, x — взаимно-простое с a, а y — с b; тогда, очевидно, z взаимно-простое и с a и с b, следовательно, и с ab (по следствию 1 теоремы 16, § 7). Этим доказана и вторая часть теоремы 54.

Но в полной системе вычетов по модулю a имеется $\varphi(a)$ значений x, взаимно-простых с a, а в полной системе вычетов по модулю b имеется $\varphi(b)$ значений y, взаимно-простых с b; следовательно, всего $\varphi(a)\varphi(b)$ значений z, взаимно-простых с ab. Но ведь все значения z образуют полную систему вычетов по модулю ab, значит:

Следствие 1. Если $D(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$. Это непосредственно обобщается на случай нескольких сомножителей, если они попарно взаимно-простые (на основании следствия 1 теоремы 16, § 7): ведь если a — взаимно-простое с b и с c, то a взаимно-простое и с bc; отсюда

$$\varphi(abc) = \varphi(a)\varphi(bc);$$

а если b и c взаимно-простые, то:

$$\varphi(bc) = \varphi(b)\varphi(c),$$

следовательно:

$$\varphi(abc) = \varphi(a)\varphi(b)\varphi(c)$$

и т. д.

Если данное число m разложено на простые множители $m = p^{\alpha}q^{\beta}r^{\gamma}\ldots$, то $p^{\alpha}, q^{\beta}, r^{\gamma}, \ldots$ попарно взаимно-простые; следовательно:

$$\varphi(m) = \varphi(p^{\alpha})\varphi(q^{\beta})\varphi(r^{\gamma})\ldots$$

Применяя формулу (60), получим:

Следствие 2. Для любого целого $m > 0$ имеем:

$$\varphi(m) = p^{\alpha-1}(p-1)q^{\beta-1}(q-1)r^{\gamma-1}(r-1)\ldots =$$
$$= m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots \qquad (61)$$

Пример: $60 = 2^2 \cdot 3 \cdot 5$; следовательно:

$$\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$$

Заметим, что $\varphi(m)$ всегда четное число, за исключением случаев, когда $m = 1$ и $m = 2$.

Всякий делитель числа m по формуле (14) § 16 имеет вид:

$$d = p^{\varkappa} q^{\lambda} r^{\mu} \ldots,$$

где $\varkappa$ может иметь значения $0, 1, 2, \ldots \alpha$; λ может иметь значения $0, 1, 2, \ldots \beta$ и т. д. Построим такое произведение

$$[1 + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^{\alpha})]\,[1 + \varphi(q) + \varphi(q^2) + \ldots + \varphi(q^{\beta})] \ldots \quad (62)$$

Перемножив эти суммы по обычному правилу умножения многочленов, найдем:

$$\sum_{\varkappa, \lambda, \mu, \ldots} \varphi(p^{\varkappa})\,\varphi(q^{\lambda})\,\varphi(r^{\mu}) \ldots = \sum_{\varkappa, \lambda, \mu, \ldots} \varphi(p^{\varkappa} q^{\lambda} r^{\mu} \ldots) = \sum_{d} \varphi(d),$$

где сумма берется по всем делителям d числа m.

С другой стороны, имеем:

$$1 + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^{\alpha}) = 1 + p - 1 + p^2 - p + \ldots + p^{\alpha} - p^{\alpha - 1} = p^{\alpha};$$

точно так же:

$$1 + \varphi(q) + \varphi(q^2) + \ldots + \varphi(q^{\beta}) = q^{\beta} \text{ и т. д.}$$

Отсюда получаем, что выражение (62) имеет значение:

$$p^{\alpha} q^{\beta} r^{\gamma} \ldots = m.$$

Итак:

Теорема 55. Если d пробегает все делители данного числа $m > 0$, то

$$\sum_{d} \varphi(d) = m. \quad (63)$$

Это — *формула Гаусса.*

§ 36. Определим еще одну арифметическую функцию — так называемую *функцию Мебиуса* (Moebius) следующим образом: $\mu(1) = \mu_1 = 1$; если $m = p^{\alpha} q^{\beta} r^{\gamma} \ldots$ разложение m на простые множители и хоть один из показателей $\alpha, \beta, \gamma, \ldots > 1$ (т. е. если m делится на некоторый квадрат > 1), то $\mu(m) = 0$. Если же $m = p_1 p_2 \ldots p_{\rho}$, где $p_1, p_2, \ldots p_{\rho}$ все различные простые числа, то $\mu(m) = \mu_m = (-1)^{\rho}$.

Таким образом, если $m = p^{\alpha} q^{\beta} r^{\gamma} \ldots$ и ρ — число различных простых чисел $p, q, r, \ldots$, то мы получим (если d пробегает все делители числа m):

$$\sum_{d} \mu_d = \mu_1 + (\mu_p + \mu_q + \mu_r + \ldots) + (\mu_{pq} + \mu_{pr} + \mu_{qr} + \ldots) +$$

$$+ (\mu_{pqr} + \ldots) + \ldots = 1 - \rho + \binom{\rho}{2} - \binom{\rho}{3} + \ldots = (1 - 1)^{\rho} = 0.$$

Только при $m = 1$ $\sum_{d} \mu_d = \mu_m = \mu_1 = 1.$

Итак:

Теорема 56. Для всякого целого числа $m > 1$ $\sum_d \mu_d = 0$; при $m = 1$ $\sum_d \mu_d = 1$. (d пробегает все делители числа m).

Выведем теперь одну общую формулу, относящуюся к арифметическим функциям,— так называемую «формулу обращения» Дедекинда (Dedekind) и Лиувилля (Liouville).

Пусть $\Phi(m)$ какая-нибудь арифметическая функция; определим другую арифметическую функцию $F(m)$ следующим образом:

$$F(m) = \sum_d \Phi(d), \tag{64}$$

где d пробегает все делители числа m.

Пусть d какой-нибудь делитель числа m; напишем формулу (64) для числа $\frac{m}{d}$:

$$F\left(\frac{m}{d}\right) = \sum_\delta \Phi(\delta); \tag{65}$$

здесь δ пробегает все делители числа $\frac{m}{d}$. Умножим обе части (65) на μ_d и просуммируем относительно всех делителей d числа m; получим:

$$\sum_d \mu_d F\left(\frac{m}{d}\right) = \sum_d \sum_\delta \mu_d \Phi(\delta). \tag{66}$$

Здесь d и δ такие делители числа m, что $\frac{m}{d\delta}$ — целое число, т. е. d можно считать делителем числа $\frac{m}{\delta}$. Суммируя в правой части (66) сначала по d, а затем по δ, получим:

$$\sum_\delta \sum_d \mu_d \Phi(\delta) = \sum_\delta \left[\Phi(\delta) \sum_d \mu_d\right]. \tag{67}$$

Но по теореме 56 $\sum_d \mu_d = 0$, за исключением случая, когда $\frac{m}{\delta} = 1$, т. е. $\delta = m$. Следовательно, в правой части (67) только одно слагаемое внешней суммы не равно нулю, а именно, при $\delta = m$; оно равно $\Phi(m)$. Итак, из (66) и (67) имеем:

$$\Phi(m) = \sum_d \mu_d F\left(\frac{m}{d}\right). \tag{68}$$

Таким образом:

Теорема 57. Если арифметическая функция $F(m)$ определяется через $\Phi(m)$ формулой (64), то, обратно, функция $\Phi(m)$ тоже однозначно определяется через $F(m)$ формулой (68).

Формула (68) и есть формула Дедекинда и Лиувилля.

Обозначают: $F(m) = \int \Phi(m)$; $\Phi(m) = DF(m)$. $F(m)$ называют

числовым интегралом от $\Phi(m)$, *взятым по делителям*; $\Phi(m)$ называют *числовою производною* от $F(m)$.

Пример 1. Если $\Phi(m) = m$, то $F(m) = S(m)$ (§ 17); если $\Phi(m) = 1$, то $F(m) = \tau(m)$ (§ 16).

Пример 2. Если $F(m) = m = p^{\alpha}q^{\beta}r^{\gamma}\ldots$, то по формуле (68):

$$\Phi(m) = \sum_d \mu_d \frac{m}{d} = m - \frac{m}{p} - \frac{m}{q} - \frac{m}{r} - \ldots + \frac{m}{pq} + \frac{m}{pr} +$$

$$+ \frac{m}{qr} + \ldots - \frac{m}{pqr} - \ldots = m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots = \varphi(m)$$

(по (61), § 35).

Таким образом, мы снова вывели формулу Гаусса (§ 35, теорема 55).

§ 37. Теорема Ферма-Эйлера. Пусть m — данный модуль, а число a взаимно-простое с m. Обозначим: $\varphi(m) = \mu$. Существуют точно μ классов чисел, взаимно-простых с m; пусть $a_1, a_2, \ldots a_\mu$ — представители этих классов. Возьмем произведения:

$$a_1a,\ a_2a,\ \ldots\ a_\mu a. \tag{69}$$

Все они тоже взаимно-простые с m (см. § 7, следствие 1 из теоремы 16) и никакие два из них не сравнимы друг с другом по модулю m, так как из $a_\kappa a \equiv a_\lambda a$ получается (см. § 33, следствие 2 из теоремы 50) $a_\kappa \equiv a_\lambda \pmod{m}$, а числа $a_1, a_2, \ldots a_\lambda$ несравнимы по модулю m. Следовательно, числа (69) — тоже представители всех классов чисел, взаимно-простых с m, значит, каждое из них сравнимо с одним и только с одним из чисел $a_1, a_2, \ldots a_\mu$. Таким образом, мы имеем μ сравнений по модулю m:

$$a_1a \equiv a_\alpha,\quad a_2a \equiv a_\beta,\ \ldots\ a_\mu a \equiv a_\delta;$$

здесь $a_\alpha, a_\beta, \ldots a_\delta$ — все числа $a_1, a_2, \ldots a_\mu$ только в каком-нибудь ином порядке. Перемножив все эти сравнения (по теореме 49, § 33), получим:

$$a_1a_2\ \ldots\ a_\mu \cdot a^\mu \equiv a_\alpha a_\beta\ \ldots\ a_\delta \pmod{m}. \tag{70}$$

Но $a_\alpha a_\beta \ldots a_\delta = a_1a_2 \ldots a_\mu$ (так как произведение не меняется от перестановки сомножителей), и на это произведение можно сократить обе части сравнения (70) (по следствию 2 из теоремы 50, § 33); получим (написав снова $\varphi(m)$ вместо μ):

Теорема 58. Если a взаимно-простое с m, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{71}$$

Частный случай. Если p — простое и a не делится на p, то

$$a^{p-1} \equiv 1 \pmod{p}, \tag{72}$$

так как $\varphi(p) = p - 1$.

Этот частный случай нашел Ферма (в XVII ст.); его доказал и обобщил Эйлер (в XVIII ст.). Поэтому эта общая теорема 58 и называется теоремой Ферма-Эйлера.

Пример 1. Пусть $m = 7$; имеем: $2^6 = 64 \equiv 1 \pmod{7}$; $3^6 = 729 \equiv 1 \pmod{7}$.

Пример 2. Пусть $m = 12$; $\varphi(12) = 4$; имеем: $5^4 = 625 \equiv \equiv 1 \pmod{12}$; $7^4 = 2401 \equiv 1 \pmod{12}$.

Другое доказательство теоремы Ферма-Эйлера. Пусть a — взаимно-простое с m; возьмем ряд степеней a: a, a^2, a^3, ... Их бесчисленное множество и все они — взаимно-простые с m. Но ведь имеется всего только $\varphi(m)$ классов чисел, взаимно-простых с m, следовательно, все степени a не могут быть несравнимыми по модулю m. Пусть $a^{\varkappa} \equiv a^{\lambda} \pmod{m}$ и $\varkappa > \lambda$; в таком случае это сравнение можно сократить на a^{λ} (следствие 2 из теоремы 50, § 33) и мы получим:

$$a^{\varkappa-\lambda} \equiv 1 \pmod{m}.$$

Следовательно, между степенями a имеются такие, которые сравнимы с 1 по модулю m. Пусть n такой *наименьший положительный* показатель, что

$$a^n \equiv 1 \pmod{m};$$

число n называется *показателем, к которому принадлежит a по модулю m*. Пусть еще: $a^{n_1} \equiv 1 \pmod{m}$, $n_1 > n$; деля n_1 на n, найдем (§ 1, теоремы 1):

$$n_1 = nq + r; \quad 0 \leqq r < n.$$

Следовательно:

$$1 \equiv a^{n_1} \equiv a^{nq+r} = a^{nq} \cdot a^r \equiv a^r \pmod{m}.$$

т. е.

$$a^r \equiv 1 \pmod{m}.$$

Но $r < n$, а n — наименьший положительный показатель, для которого $a^n \equiv 1 \pmod{m}$; значит, $r = 0$, и n_1 делится на n.

Если теперь: $a^{\varkappa} \equiv a^{\lambda} \pmod{m}$, $\varkappa > \lambda$, то

$$a^{\varkappa-\lambda} \equiv 1 \pmod{m},$$

следовательно, $\varkappa - \lambda$ делится на n, или $\varkappa \equiv \lambda \pmod{n}$.

Очевидно, что и обратно: если $\varkappa - \lambda$ делится на n, то $a^{\varkappa-\lambda} \equiv \equiv 1 \pmod{m}$; умножив обе части этого сравнения на a^{λ}, получим:

$$a^{\varkappa} \equiv a^{\lambda} \pmod{m}.$$

Итак:

Теорема 59. Для всякого числа a, взаимно-простого с m, найдется такое натуральное число n (показатель, к которому принадлежит a по модулю m), что: 1) $a^n \equiv 1 \pmod{m}$, 2) $a^{\varkappa} \equiv a^{\lambda} \pmod{m}$ тогда и только тогда, когда $\varkappa \equiv \lambda \pmod{n}$.

Отсюда следует, что никакие две степени из ряда

$$a^0 = 1, \ a, \ a^2, \ a^3, \ \ldots \ a^{n-1} \tag{73}$$

не сравнимы друг с другом по модулю m (или, как говорят, все степени (73) *различны* по модулю m), так как при $0 \leqq \varkappa < n$, $0 \leqq \lambda < n$, $\varkappa \neq \lambda$ $\varkappa - \lambda$ не может делиться на n. Следовательно,

степени (73) являются представителями различных классов по модулю m, взаимно-простых с m. Если $n = \varphi(m)$, то теорема 58 уже доказана. Если же $n < \varphi(m)$, то, значит, имеется еще число b, взаимно-простое с m и не сравнимое ни с одной из степеней (73). Возьмем произведения:

$$b,\ ba,\ ba^2,\ \ldots\ ba^{n-1}; \tag{74}$$

все они взаимно-простые с m и различны по модулю m, так как из $ba^{\varkappa} \equiv ba^{\lambda} \pmod m$ следует (следствие 2 из теоремы 50, § 33): $a^{\varkappa} \equiv a^{\lambda} \pmod m$, что́ неверно. Никакое произведение (74) не сравнимо и с степенью (73), ибо из

$$ba^{\varkappa} \equiv a^{\lambda} \pmod m$$

при $\lambda > \varkappa$ вытекает: $b \equiv a^{\lambda-\varkappa} \pmod m$, а при $\lambda < \varkappa$ следует (умножая на $a^{n-\varkappa}$): $b \equiv a^{n+\lambda-\varkappa} \pmod m$, но ведь b не сравнимо ни с какой степенью a.

Отсюда следует, что числа (73) и (74) являются представителями различных классов по модулю m, взаимно-простых с m; следовательно, $\varphi(m) \geqq 2n$. Если $\varphi(m) = 2n$, то теорема 58 доказана, ибо тогда $a^{\varphi(m)} = a^{2n} \equiv 1 \pmod m$. Если же $\varphi(m) > 2n$, то имеется еще по крайней мере один класс чисел, взаимно-простых с m.

Пусть c — представитель этого класса; тогда берем произведения:

$$c,\ ca,\ ca^2,\ \ldots\ ca^{n-1} \tag{75}$$

и доказываем, что эти n чисел — представители новых n классов чисел, взаимно-простых с m, а следовательно, $\varphi(m) \geqq 3n$.

Для этого следует доказать, что: 1) все числа (75) различны по модулю m; 2) числа (75) не сравнимы с числами (73); 3) числа (75) не сравнимы с числами (74). Но 1) и 2) доказывается так же, как и для ряда (74). Докажем 3). Пусть

$$ca^{\varkappa} \equiv ba^{\lambda} \pmod m;$$

отсюда при $\lambda > \varkappa$ следует: $c \equiv ba^{\lambda-\varkappa} \pmod m$, а при $\lambda < \varkappa$ $c \equiv ba^{n+\lambda-\varkappa} \pmod m$. Оба раза получается, что c сравнимо с одним из чисел (74), а это неверно; т. е. 3) доказано.

Подобно же продолжаем и далее.

Таким образом, при $kn < \varphi(m)$ мы выводим, что $(k+1)n \leqq \varphi(m)$. Но этот процесс должен закончиться, так как все наши числа целые и $\varphi(m)$ конечно. Следовательно, при некотором натуральном k будет $\varphi(m) = kn$, и теорема 58 доказана.

Из предыдущих рассуждений следует такое дополнение к теореме 59:

Показатель, к которому принадлежит a по модулю m, есть делитель числа $\varphi(m)$.

Следствие из теоремы 58. Если p — простое, а a — любое целое число, то

$$a^p \equiv a \pmod p. \tag{76}$$

Ибо при a, не делящемся на p, мы получим (76) умножая обе части (72) на a. Если же a делится на p, то сравнение (76) очевидно: каждая его часть сравнима с нулем по модулю p.

Заметим, что и обратно: при a, не делящемся на p, из (76) следует (72).

§ 38. Тождественные и условные сравнения. Если в сравнение входят неопределенные величины (буквы), то подобно тому, как в равенствах, могут быть два случая:

1. Сравнение остается верным при всех (целых) значениях входящих в него букв; эти буквы — *переменные*. Данный случай соответствует тождеству.

2. Сравнение верно только при некоторых определенных значениях входящих в него букв; эти значения надо найти; буквы — *неизвестные*. Данный случай соответствует уравнению. Такое сравнение назовем *условным*.

Однако аналогия с равенствами здесь неполная: во-первых, кроме двух частей сравнения, здесь есть еще и модуль, который тоже может быть неизвестным. Но такое сравнение мы в дальнейшем не будем рассматривать. Во-вторых, относительно модуля m у нас всего только m различных чисел, или различных классов. Таким образом, чтобы найти все решения данного сравнения, нужно каждому неизвестному придать только m различных значений, т. е. произвести только конечное число испытаний, так как из теоремы 51 (§ 33) следует, что вместе с числом a и все числа, сравнимые с a по данному модулю, удовлетворяют нашему сравнению или все не удовлетворяют ему.

Обе части сравнения — целые рациональные функции от букв (неизвестных или переменных) с целыми коэффициентами. Если мы перенесем все члены в сравнении в левую часть так, чтобы с правой оказался нуль, то получим сравнение такого вида:

$$f(x,\ y,\ z,\ \ldots) \equiv 0 \pmod{m}, \tag{77}$$

где $f(x,\ y,\ z,\ \ldots)$ целая рациональная функция от $x,\ y,\ z,\ \ldots$ с целыми коэффициентами. Но здесь имеется отличие от равенств: если равенство $f(x,\ y,\ z,\ \ldots) = 0$ есть тождество, т. е. верно для всех значений $x,\ y,\ z,\ \ldots$ то все коэффициенты левой части должны быть равны нулю; очевидно и обратное. В сравнении же (77), конечно, если все коэффициенты левой части делятся на m, то всякие целые значения переменных $x,\ y,\ z,\ \ldots$ этому сравнению удовлетворяют. Однако не обратно, как следует из такого примера: мы видели, что сравнение (76) удовлетворяется всяким целым значением a, но ведь это сравнение вида $a^p - a \equiv 0 \pmod{p}$; в левой его части коэффициенты 1 и -1 не делятся на p.

В дальнейшем мы будем считать *тождественным сравнением* такое сравнение вида (77), в котором все коэффициенты левой части делятся на m. Таким образом, бывают сравнения удовлетворяющиеся любыми (целыми) значениями переменных, но не тождественные.

Условные сравнения бывают с одним, с двумя, с тремя и т. д. неизвестными. Наивысшая степень неизвестного в условном сравнении (после всех его упрощений) называется *степенью сравнения*. Мы рассмотрим сравнения только 1-й и 2-й степени с одним неизвестным. Решения сравнения называются его *корнями*.

Как мы уже говорили, корни сравнения тоже определяются по данному модулю m, т. е. вместе с данным корнем x_0 все числа класса, к которому принадлежит x_0, тоже являются корнями того же сравнения. Такие корни мы не считаем отличными от x_0; иными словами, мы считаем корнем весь класс, представителем которого является x_0. Следовательно, если мы говорим, что x_1 и x_2 — различные корни данного сравнения (по модулю m), то это значит, что x_1 и x_2 не сравнимы друг с другом по модулю m.

§ 39. Сравнения 1-й степени. Общий вид такого сравнения:

$$ax \equiv b \pmod{m}, \tag{78}$$

где a и b — данные (целые) коэффициенты.

Рассмотрим сначала случай, когда $D(a, m) = 1$. Пусть x пробегает полную систему вычетов по модулю m; в таком случае и ax тоже пробегает полную систему вычетов по модулю m, так как из сравнения $ax_\varkappa \equiv ax_\lambda \pmod{m}$ следует (§ 33, теорема 50, следствие 2): $x_\varkappa \equiv x_\lambda \pmod{m}$ (ср. также § 32, пример 5). При некотором единственном $x = x_0$ вычет ax_0 из этой системы принадлежит к тому же классу, что и b, т. е. $ax_0 \equiv b \pmod{m}$, и это решение $x \equiv x_0 \pmod{m}$ единственное.

Пусть теперь $D(a, m) = d > 1$; если $ax - b = my$ (т. е. делится на m), то b должно делиться на d. Следовательно, если b не делится на d, то наше сравнение (78) не имеет решений. Пусть b делится на d: $b = db_1$; обозначаем еще: $a = da_1$, $m = dm_1$; тогда (по следствию 1 из теоремы 50, § 33) сравнение (78) равносильно (т. е. удовлетворяется теми же самыми значениями неизвестных) сравнению:

$$a_1 x \equiv b_1 \pmod{m_1}. \tag{79}$$

Здесь $D(a_1, m_1) = 1$ (по теореме 10, § 4) следовательно, сравнение (79) имеет одно и только одно решение по модулю m_1: $x \equiv x_0 \pmod{m_1}$ или $x = x_0 + km_1$, где k — любое целое число. Все эти значения x удовлетворяют и сравнению (78), но только здесь мы их рассматриваем по модулю m.

Легко видеть, что при $k = 0, 1, 2, \ldots d-1$ мы получим решения:

$$x_0, \; x_0 + \frac{m}{d}, \; x_0 + 2\frac{m}{d}, \; \ldots \; x_0 + (d-1)\frac{m}{d}, \tag{80}$$

различные по модулю m, тогда как при всех других (целых) значениях k числа $x_0 + km_1 = x_0 + k\frac{m}{d}$ будут все сравнимы с числами (80) по модулю m. Следовательно, в этом случае сравнение (78) имеет d решений.

Таким образом:

Теорема 60. Сравнение 1-й степени вида (78) имеет решения тогда и только тогда, когда b делится на $d = D(a, m)$, и в этом случае — точно d решений. В частности, при $d = 1$ сравнение (78) имеет всегда и только одно решение.

Относительно практического решения сравнений заметим, что хотя конечным числом испытаний можно всегда найти все решения, однако при большом модуле m этот способ практически весьма громоздок. Мы дадим два более удобных способа.

1) Сравнение вида (78) — только иначе выраженное уравнение 1-й степени с двумя неизвестными: $ax - b = my$, или

$$ax - my = b.$$

Мы уже знаем, как решить в целых числах это уравнение при помощи алгорифма Эвклида или цепных дробей (§ 28). Мы знаем также, что если x_0 — частное решение, то общее решение есть: $x = x_0 + k\frac{m}{d}$, где $d = D(a, m)$; это то же, что нам дают и формулы (80).

Пример 1. Решить сравнение

$$58x \equiv 87 \pmod{47}.$$

Сначала заменим коэффициенты их наименьшими положительными вычетами по модулю 47:

$$11x \equiv 40 \pmod{47}.$$

Затем решим сравнение $11x' \equiv 1 \pmod{47}$. Для этого по правилу § 28 применим алгорифм Эвклида к числам 47 и 11:

$$47 : 11 = 4$$
$$11 : \overline{3} = 3$$
$$3 : \overline{2} = 1$$
$$2 : \overline{1} = 2$$

Вычислим скобки Эйлера [1, 3, 4], беря в них все наши частные, кроме последнего:

	1	3	4
1	1	4	17

Очевидно, $|x'| = 17$; чтобы определить знак у x', найдем последние цифры в произведениях: $11 \cdot 17$ и $47 \cdot 4$. Они будут 7 и 8: но должно быть $11x' - 47y' = 1$, следовательно, $x' = -17$, $y' = -4$ (значение y' нам не нужно). Чтобы найти x, надо x' умножить на правую часть нашего сравнения, т. е. на 40; получим: $x = -680$, или правильнее: $x \equiv -680 \pmod{47}$. «Приведем» — 680 по модулю 47 (т. е. найдем наименьший положительный или абсолютно-наименьший вычет) и получим:

$$x \equiv 25 \pmod{47}.$$

Лучше было бы в правой части сравнения вместо 40 взять абсолютно наименьший вычет по модулю 47, т. е. —7; мы нашли бы:

$$x = (-17)(-7) = 119 \equiv 25 \pmod{47}.$$

Это решение — единственное.

Пример 2. $78x \equiv 57 \pmod{93}$; здесь $D(78, 93) = 3$; 57 делится на 3, т. е. решения имеются. Сократив на 3, найдем:

$$26x \equiv 19 \pmod{31}.$$

Сначала решим сравнение:

$$26x' \equiv 1 \pmod{31};$$

имеем: $31 : 26 = 1$ $\quad \begin{array}{ccc} & 5 & 1 \\ \hline 1 & 5 & 6 \end{array}$

$26 : \overline{5} = 5$

$5 : \overline{1} = 5$

$|x'| = 6$. В произведении $26 \cdot 6$ последняя цифра 6, а в произведении $31 \cdot 5$ последняя цифра 5, следовательно, $x' = +6$; отсюда:

$$x \equiv 6 \cdot 19 \equiv 114 \equiv -10 \pmod{31}.$$

Относительно же модуля 93 имеем три различных решения:

$$x_1 \equiv -10 \pmod{93}; \quad x_2 \equiv 21 \pmod{93}; \quad x_3 \equiv 52 \pmod{93}.$$

2) *Способ Эйлера*. Пусть в сравнении (78) a — взаимно-простое с m; тогда по теореме 58 (Ферма - Эйлера):

$$a^{\varphi(m)} = a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m};$$

$$a(a^{\varphi(m)-1} \cdot b) \equiv b \pmod{m}.$$

Следовательно,

$$x \equiv a^{\varphi(m)-1} \cdot b \qquad (81)$$

и есть корень нашего сравнения (78) (при $D(a, m) = 1$).

Недостаток этого способа тот, что при большом $\varphi(m)$ приходится возвышать a в степень с большим показателем $\varphi(m) - 1$. Вычисления упрощаются, если возводить в степень «по данному модулю», т. е. одновременно приводить результат по модулю, как мы покажем на примерах.

Пример 3. $11x \equiv 15 \pmod{24}$. Здесь $D(11, 24) = 1$. Находим: $\varphi(24) = 8$; нужно найти 11^7. Будем вместо равенств писать сравнения по модулю 24. Найдем: $11^2 = 121 \equiv 1$, следовательно, $11^4 \equiv 1$, $11^6 \equiv 1$, $11^7 \equiv 11$. Далее: $11 \cdot 15 = 165 \equiv -3$, следовательно, $x \equiv -3 \pmod{24}$.

Пример 4. $196x \equiv 77 \pmod{91}$. Приводим по модулю 91: $14x \equiv 77 \pmod{91}$. Здесь $D(14, 91) = 7$. Сократим на 7: $2x \equiv 11 \pmod{13}$; $\varphi(13) = 12$. Имеем (по модулю 13): $2^2 = 4$, $2^4 = 16 \equiv 3$, $2^8 \equiv 9$, $2^{11} = 2^8 \cdot 2^2 \cdot 2 \equiv 9 \cdot 4 \cdot 2 = 72 \equiv 7$; $7 \cdot 11 = 77 \equiv -1$. Следовательно, имеем семь решений по модулю 91: -1, 12, 25, 38, 51, 64, 77.

Заметим, что проще было бы в сравнении $2x \equiv 11 \pmod{13}$ вместо 11 взять наименьший отрицательный вычет -2; сократив на 2, мы сразу получили бы: $x \equiv -1 \pmod{13}$.

Вообще при небольших коэффициентах и модулях часто бывает возможно решить данное сравнение элементарным путем, применяя

элементарные свойства сравнений, выведенные в § 33. Покажем это на примере.

Пример 5. $39x \equiv 19 \pmod{53}$. Берем наименьшие отрицательные вычеты: $-14x \equiv -34 \pmod{53}$. Сокращаем на -2: $7x \equiv 17 \equiv$ $\equiv 17 + 53 = 70 \pmod{53}$; сокращаем на 7: $x \equiv 10 \pmod{53}$. Это и есть искомое решение.

§ 40. Теорема Вильсона. Пусть наш модуль — простое число $p > 3$. Сравнение:

$$ax \equiv 1 \pmod{p}$$

при a, не делящемся на p, имеет одно и только одно решение: $x \equiv b \pmod{p}$; поэтому

$$ab \equiv 1 \pmod{p}. \tag{82}$$

Числа a и b можно взять из ряда: $1, 2, 3, \ldots p-1$; следовательно, каждому числу a из этого ряда соответствует определенное число b из того же ряда такое, что выполнено сравнение (82).

Посмотрим, может ли быть $b = a$; тогда бы мы имели:

$$a^2 \equiv 1 \pmod{p},$$

или:

$$a^2 - 1 = (a-1)(a+1) \equiv 0 \pmod{p}.$$

Следовательно (по теореме 19 в § 10), один из множителей $a-1$ или $a+1$ делится на p (оба вместе они не могут делиться на p, так как их разность $= 2$ — не делится на p). Таким образом, или $a \equiv 1 \pmod{p}$, или $a \equiv -1 \pmod{p}$, т. е. или $a = 1$, или $a = p-1$. Во всех остальных случаях, т. е. когда $a = 2, 3, \ldots p-2$, всегда $b \neq a$ и b — тоже число того же ряда. Т. е. все эти числа 2, $3, \ldots p-2$ распределяются по парам таких чисел a и b, что $ab \equiv 1 \pmod{p}$; таких пар всего $\frac{p-3}{2}$. Перемножив почленно $\frac{p-3}{2}$ сравнений (82), получим:

$$2, 3 \ldots (p-2) \equiv 1 \pmod{p}.$$

Имеем кроме того: $p - 1 \equiv -1 \pmod{p}$. Перемножив почленно эти два сравнения, найдем:

$$(p-1)! \equiv -1 \pmod{p}. \tag{83}$$

Эта формула и выражает теорему Вильсона.

Мы предположили, что $p > 3$; но легко непосредственно убедиться, что формула (83) верна и для $p = 2$ и для $p = 3$:

$$1! \equiv -1 \pmod{2}; \quad 2! \equiv -1 \pmod{3}.$$

Если p не простое, то формула (83) неверна, ибо в этом случае $(p-1)!$ имеет с p общий множитель > 1, а потому $(p-1)! + 1$ не может делиться на p.

Итак:

Теорема 61. Если p — простое число, то в этом и только в этом случае $(p-1)! + 1$ делится на p.

Таким образом, формула (83) характерна для простых чисел и, пользуясь ею, можно было бы узнавать, простое ли данное число. Но к сожалению, этот способ совершенно непрактичный, так как даже для сравнительно небольших p произведение $(p-1)!$ — огромное число.

§ 41. Десятичные дроби. Пусть дана обычная правильная дробь $\frac{a}{b}$; $0 < a < b$ — целые, взаимно-простые числа. Предположим сначала, что b и 10 — взаимно-простые. Обратим эту дробь в десятичную; для этого делим $10a$ на b:

$$10a = ba_1 + r_1; \quad 0 < r_1 < b.$$

Теперь делим $10r_1$ на b:

$$10r_1 = ba_2 + r_2; \quad 0 < r_2 < b.$$

Далее делим $10r_2$ на b:

$$10r_2 = ba_3 + r_3; \quad 0 < r_3 < b; \text{ и т. д.}$$

$$\cdots\cdots\cdots\cdots$$

$$10r_{m-1} = ba_m + r_m; \quad 0 < r_m < b.$$

Ни один остаток r_m не равен нулю, ибо $10r_{m-1}$ и b взаимно-простые.

Имеем далее:

$$\frac{a}{b} = \frac{a_1}{10} + \frac{r_1}{10b};$$

$$\frac{r_1}{b} = \frac{a_2}{10} + \frac{r_2}{10b};$$

$$\cdots\cdots$$

$$\frac{r_{m-1}}{b} = \frac{a_m}{10} + \frac{r_m}{10b}.$$

Отсюда найдем:

$$\frac{a}{b} = \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_m}{10^m} + \frac{r_m}{10^m b}; \tag{84}$$

$$\lim_{m\to\infty} \frac{r_m}{10^m b} = 0,$$

следовательно, ряд (84) при $m \to \infty$ будет сходящимся. Умножив обе части (84) на $10^m b$ и перенеся последний член в левую часть, получим:

$$10^m a - r_m = (a_1 10^{m-1} + a_2 10^{m-2} + \ldots + a_m) b. \tag{85}$$

До сих пор m было произвольным натуральным числом; пусть теперь m — показатель, к которому принадлежит 10 по модулю b (§ 37, теорема 59). Тогда $10^m \equiv 1 \pmod{b}$ и, написав (85) как сравнение по модулю b, получим:

$$a - r_m \equiv 0 \pmod{b}.$$

Но a и r_m — целые положительные числа $< b$; следовательно, $a = r_m$. Но тогда, продолжив деления, найдем: $r_1 = r_{m+1}$, $r_2 = r_{m+2}$, ...,

а также: $a_1 = a_{m+1}$, $a_2 = a_{m+2}$, ..., т. е. дробь $0, a_1a_2a_3 \ldots$ *) будет периодическая с периодом: $a_1a_2 \ldots a_m$. Докажем что этот период наименьший **).

Пусть наименьший период имеет m' цифр; можно написать (85), заменив m на m':

$$10^{m'}a - r_{m'} = (a_1 10^{m'-1} + a_2 10^{m'-2} + \ldots + a_{m'})\,b.$$

Но здесь $r_{m'} = a$; следовательно:

$$(10^{m'} - 1)\,a \equiv 0 \pmod{b}.$$

Но $D(a, b) = 1$; следовательно (по теореме 15):

$$10^{m'} \equiv 1 \pmod{b};$$

следовательно (§ 37, теорема 59) m' делится на m. Но $m' \leqq m$; значит, $m' = m$, и найденный нами период наименьший.

Мы видим, что m зависит только от знаменателя в нашей дроби (и, конечно, от основания нашей системы счисления, т. е. от числа 10). Чтобы найти m при данном b, надо $10 - 1 = 9$, $100 - 1 = 99$, $1000 - 1 = 999$, и т. д. делить на b, пока не получим деления без остатка (а его мы непременно получим, если $D(b, 10) = 1$). Число девяток в этом делении и равно искомому числу m. Практически мы сначала пишем столько девяток, чтобы полученное число было больше, чем b, а затем делим как десятичную дробь, приписывая к остатку каждый раз не 0, а 9.

Пример 1. $b = 37$; делим:

$$\begin{array}{r|l} 99 & 37 \\ \underline{74} & \overline{027} \\ 259 & \\ \underline{259} & \end{array}$$

В частном три цифры (считая и 0, который соответствует первой девятке); следовательно, $m = 3$.

Пример 2. $b = 13$; делим:

$$\begin{array}{r|l} 99 & 13 \\ \underline{91} & \overline{076923} \\ \underline{89} & \\ 78 & \\ \underline{119} & \\ 117 & \\ \underline{29} & \\ 26 & \\ \underline{39} & \\ 39 & \end{array}$$

Следовательно, $m = 6$.

---

*) Легко видеть, что $a_1, a_2, a_3, \ldots$ все «цифры», т. е. однозначные числа; это следует из того, что $b > a$, $b > r_1$, $b > r_2$, ...

**) Например, периодическую дробь 0, (47) можно представить и так: 0, (4747), или так: 0, (474747), и т. д. Здесь и 4747 и 474747 — периоды, но не наименьшие; наименьший период здесь 47.

Если дробь $\frac{a}{b}$ неправильная, т. е. $a > b$, то надо сначала выделить из нее целую часть.

Пусть теперь дробь попрежнему несократима, но b и 10 не взаимно-простые, т. е. b имеет множители 2 или 5, или и 2 и 5. Пусть $b = 2^\alpha \cdot 5^\beta \cdot b_1$, где $D(b_1, 10) = 1$. Обозначим через γ наибольшее из чисел α и β и возьмем число:

$$\frac{10^\gamma a}{b} = \frac{a_1}{b_1};$$

дробь $\frac{a_1}{b_1}$ — несократима и знаменатель ее b_1 — взаимно-простой с 10. Обратим эту дробь в десятичную периодическую по предыдущему правилу:

$$\frac{a_1}{b_1} = k, (c_1 c_2 \ldots c_m).$$

здесь k — целая часть, а $c_1 c_2 \ldots c_m$ — период дроби. Чтобы получить дробь $\frac{a}{b}$, нужно $\frac{a_1}{b_1}$ разделить на 10^γ, т. е. перенести запятую на γ знаков влево; получим:

$$\frac{a}{b} = l, b_1 b_2 \ldots b_\gamma (c_1 c_2 \ldots c_m).$$

Это — смешанная периодическая дробь; между запятой и периодом находится γ цифр.

Рассмотрим теперь обратную задачу: найти обыкновенную дробь, представляющую значение данной периодической дроби. Заметим, что бесконечная десятичная дробь — не что иное, как бесконечный сходящийся ряд, и нам нужно найти его сумму.

Пусть дана чистая периодическая дробь: $x = k, (a_1 a_2 \ldots a_m)$; следовательно:

$$x = k + \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_m}{10^m}\right) + \frac{1}{10^m}\left(\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_m}{10^m}\right) + $$
$$+ \frac{1}{10^{2m}}\left(\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_m}{10^m}\right) + \ldots$$

или:

$$x = k + (10^{m-1} a_1 + 10^{m-2} a_2 + \ldots + a_m)\left(\frac{1}{10^m} + \frac{1}{10^{2m}} + \frac{1}{10^{3m}} + \ldots\right).$$

В последних скобках — сумма членов убывающей геометрической прогрессии с первым членом $= \frac{1}{10^m}$ и со знаменателем $= \frac{1}{10^m}$. Эта сумма равна:

$$\frac{1}{10^m} : \left(1 - \frac{1}{10^m}\right) = \frac{1}{10^m - 1};$$

число $10^m - 1$ изображается m девятками. Итак, имеем:

$$x = k + \frac{10^{m-1} a_1 + 10^{m-2} a_2 + \ldots + a_m}{10^m - 1}. \qquad (86)$$

Таким образом, *чтобы обратить чистую периодическую дробь в обыкновенную, надо период дроби сделать числителем, а в знаменателе написать столько девяток, сколько цифр в периоде, и полученную дробь прибавить к целой части.*

Пусть теперь дана смешанная периодическая дробь: $x = k, b_1 b_2 \dots b_\gamma (c_1 c_2 \dots c_m)$; ее можно представить так:

$$x = [k b_1 b_2 \dots b_\gamma,\ (c_1 c_2 \dots c_m)] : 10^\gamma = \left[k b_1 b_2 \dots b_\gamma \frac{c_1 c_2 \dots c_m}{10^m - 1}\right] : 10^\gamma =$$

$$= k + \frac{b_1 10^{\gamma-1} + b_2 10^{\gamma-2} + \dots + b_\gamma}{10^\gamma} + \frac{c_1 10^{m-1} + c_2 10^{m-2} + \dots + c_m}{10^\gamma \cdot (10^m - 1)};$$

или:

$$x = k + [(b_1 10^{m+\gamma-1} + b_2 10^{m+\gamma-2} + \dots + b_\gamma 10^m +$$

$$+ c_1 10^{m-1} + \dots + c_m) - (b_1 10^{\gamma-1} + b_2 10^{\gamma-2} + \dots + b_\gamma)] \cdot \frac{1}{10^\gamma \cdot (10^m - 1)}.$$

Отсюда получаем такое правило: чтобы обратить смешанную периодическую дробь в обыкновенную, надо из числа, стоящего между запятой и вторым периодом (т. е. из числа $b_1 b_2 \dots b_\gamma c_1 c_2 \dots c_m$), вычесть число, стоящее между запятой и первым периодом (т. е. число $b_1 b_2 \dots b_\gamma$), и эту разность сделать числителем; в знаменателе написать столько девяток, сколько цифр в периоде, и после них — столько нулей, сколько цифр между запятой и первым периодом, и эту дробь прибавить к целой части.

Пример 1. Дана чистая периодическая дробь:

$$2,(435) = 2\frac{435}{999} = 2\frac{145}{333}.$$

Пример 2. Дана смешанная периодическая дробь:

$$5{,}38(4) = 5\frac{384 - 38}{900} = 5\frac{346}{900} = 5\frac{173}{450}.$$

Замечание. Можно сразу обратить периодическую дробь в обыкновенную неправильную дробь (не выделяя целой части); для этого следует цифры целой части считать как цифры, стоящие до периода, и применить правило для обращения смешанной периодической дроби в обыкновенную. При этом при построении знаменателя цифры целой части не следует учитывать. Например:

$$2,(435) = \frac{2435 - 2}{999} = \frac{2433}{999} = \frac{811}{333};$$

$$5{,}38(4) = \frac{5384 - 538}{900} = \frac{4846}{900} = \frac{2423}{450}.$$

§ 42. Признаки делимости. Проблема построения признаков делимости состоит в следующем: пусть N данное натуральное число, а d — данный делитель (тоже натуральное число); надо

построить арифметическую функцию $f(N)$, имеющую только целые значения, с такими условиями:

1) N и $f(N)$ одновременно делятся или одновременно не делятся на d;

2) $|f(N)| < N$, кроме случаев, когда N достаточно мало;

3) при данном N функция $f(N)$ вычисляется более или менее просто.

Если требуется определить, делится ли N на d, то вычисляем $f(N)$; если $|f(N)|$ еще довольно велико, то вычисляем $f(|f(N)|)$ и т. д., пока не получим достаточно малого числа, так что можно непосредственно видеть, делится ли оно на d. Заметим еще, что нам достаточно найти признаки делимости только на числа $d = p^\alpha$, где p — простое число, так как по следствию из теоремы 17 в § 8 число N делится на $d = p^\alpha q^\beta r^\gamma \ldots (p, q, r, \ldots$ — различные простые числа) тогда и только тогда, когда оно делится на p^α, на q^β, на r^γ и т. д.

Переходим к способам построения функции $f(N)$.

Способ Паскаля. Всякое натуральное число N в десятичной системе счисления имеет вид:

$$N = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^n a_n,$$

где $a_0, a_1, a_2, \ldots a_n$ — «цифры», т. е. целые числа $\geqq 0$ и < 10.

Исследуя делимость или неделимость этого числа на d, можно заменить его числом M, сравнимым с N по модулю d, при этом удобнее взять M как можно меньшим. Построим M, заменяя в N степени числа 10 их абсолютно наименьшими вычетами по модулю d. Пусть для 10^k абсолютно наименьший вычет по модулю d есть c_k; тогда:

$$M = a_0 + a_1c_1 + a_2c_2 + \ldots + a_nc_n;$$
$$N \equiv a_0 + a_1c_1 + a_2c_2 + \ldots + a_nc_n \pmod{d}.$$

Заметим, что d может быть любым натуральным числом.

Здесь $M = f(N) \equiv N \pmod{d}$; это — больше, чем нам требуется: для нас важно только, что M и N одновременно делятся или не делятся на d.

Частные случаи. 1. $d = 2$. Здесь $c_k = 0$ $(k = 1, 2, \ldots)$; следовательно, $N \equiv a_0 \pmod 2$; это — известный признак делимости на 2.

2. $d = 3$. Здесь $c_k = 1$ $(k = 1, 2, \ldots)$; следовательно, $N \equiv a_0 + a_1 + \ldots + a_n \pmod 3$; это — тоже известный признак делимости на 3.

3. $d = 4$. Здесь $c_1 = \pm 2$, $c_2 = c_3 = \ldots = 0$; следовательно, $N \equiv a_0 \pm 2a_1 \pmod 4$.

Этот признак делимости на 4 удобнее обычного (что две последние цифры образуют число, делящееся на 4).

Примеры: 1) 76 делится на 4, ибо $6 + 2 \cdot 7 = 20$, или $6 - 2 \cdot 7 = -8$ делится на 4; 2) 366 не делится на 4, ибо $6 + 12 = 18$ или $6 - 12 = -6$ не делится на 4.

4. $d = 6$. Здесь $c_1 = c_2 = c_3 = \ldots = -2$; следовательно, $N \equiv a_0 - 2(a_1 + a_2 + \ldots + a_n) \pmod 6$.

Пример. 138 делится на 6, ибо $8 - 2 \cdot (1 + 3) = 0$.

5. $d = 7$. Здесь $c_1 = 3$, $c_2 = 2$, $c_3 = -1$, $c_4 = -3$, $c_5 = -2$, $c_6 = 1$, $c_7 = 3$ и т. д. периодически; следовательно, $N \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + \ldots \pmod 7$.

Примеры: 1) 343 делится на 7, ибо $3 + 3 \cdot 4 + 2 \cdot 3 = 21$ — делится на 7; 2) 24829 делится на 7, ибо $9 + 2 \cdot 3 + 8 \cdot 2 - 4 - 2 \cdot 3 = 21$ — делится на 7.

6. $d = 8$. Здесь $c_1 = 2$, $c_2 = \pm 4$, $c_3 = c_4 = \ldots = 0$; следовательно, $N \equiv a_0 + 2a_1 \pm 4a_2 \pmod 8$.

Пример. 5792 делится на 8, ибо $2 + 2 \cdot 9 - 4 \cdot 7 = -8$ делится на 8.

7. $d = 11$. Здесь $c_1 = -1$, $c_2 = +1$, $c_3 = -1$, $c_4 = +1$ и т. д., следовательно, $N \equiv a_0 - a_1 + a_2 - a_3 + \ldots \pmod{11}$.

Пример. 5841 делится на 11, ибо $1 - 4 + 8 - 5 = 0$.

Способ Жбиковского *). В этом способе требуется чтобы делитель d был взаимно-простой с основанием счисления, т. е. с числом 10, т. е. не делился ни на 2, ни на 5. В таком случае всегда имеет решение сравнение

$$10M \equiv N \pmod d \qquad (87)$$

с неизвестным M.

Из этого сравнения видно, что если N делится на d, то и $10\,M$ тоже делится на d. Но $D(d, 10) = 1$, следовательно (по теореме 15, § 8), M делится на d.

Обратно, если M делится на d, то, очевидно, и N делится на d. Мы и берем: $f(N) = M$. Находим M так: сначала решим сравнение: $10k \equiv 1 \pmod d$; тогда $M \equiv kN \pmod d$ и будет решением сравнения (87). Но мы имеем:

$$kN = k(a_0 + 10a_1 + 10^2 a_2 + \ldots + 10^n a_n) = ka_0 + 10ka_1 + \\ + 10k \cdot 10a_2 + \ldots + 10k10^{n-1} a_n \equiv (ka_0 + a_1) + \\ + 10a_2 + \ldots + 10^{n-1} a_n \pmod d.$$

Поэтому мы и берем:

$$M = ka_0 + a_1 + 10a_2 + \ldots + 10^{n-1} a_n.$$

Очевидно, что при большом числе N M меньше, чем N приблизительно в 10 раз. С M мы поступаем дальше так же, как с N.

Заметим, что k зависит только от d, но не от N, и определяется однозначно по модулю d; за k можно взять наименьший положительный или абсолютно наименьший вычет. Заметим еще, что M не сравнимо вообще с N по модулю d; они только одновременно делятся или не делятся на d.

Частные случаи. 1. $d = 3$. Здесь $k = 1$; следовательно, $M = a_0 + a_1 + 10a_2 + 10^2 a_3 + \ldots$ Но взяв M вместо N, мы по-

---

*) А. К. Жбиковский. Относительно делимости чисел. «Вестник математических наук», т. 1, № 1 (1861), стр. 5—6. См. также Н. В. Бугаев. К теории делимости чисел. Математический сборник, т. 8 (1877), стр. 501—505.

добно же найдем: $kM \equiv M_1 = a_0 + a_1 + a_2 + 10a_3 + \ldots$, и т. д. Получаем по существу обычный признак делимости на 3.

2. $d = 7$. Здесь $k = 5$ или $k = -2$; следовательно, $M = 5a_0 + a_1 + 10a_2 + \ldots$, или: $M = a_1 - 2a_0 + 10a_2 + \ldots$.

Примеры: 1) $N = 343$, $M = 34 + 15 = 49$ или $M = 34 - 6 = 28$. 2) $N = 24829$; находим последовательно: $2482 + 45 = 2527$; $252 + 35 = 287$; $28 - 14 = 14$ (лучше было бы от числа 2527 просто откинуть семерку и взять 252; мы бы нашли: $25 - 4 = 21$).

3. $d = 11$. Здесь $k = -1$ (или 10); $M = -a_0 + a_1 + 10a_2 + 10^2a_3 + \ldots$ Но взяв M вместо N, найдем далее: $M = a_0 - a_1 + a_2 + 10a_3 + \ldots$, и т. д. — получаем по существу тот же признак, что и способом Паскаля.

4. $d = 13$. Здесь $k = 4$; $M = 4a_0 + a_1 + 10a_2 + 10^2a_3 + \ldots$

Пример. $N = 182$; строим: $M = 18 + 8 = 26$ — делится на 13.

Заметим, что иногда уже внешний вид числа N позволяет упростить вопрос о его делимости на d. Если начало или конец числа N (при d — взаимно-простом с 10) образует число, делящееся на d, то его можно просто откинуть. Например, чтобы определить, делится ли число 358542 на 7, можно откинуть две первые и две последние его цифры, так как 35 и 42 делятся на 7, и исследовать число 85, которое, очевидно, не делится на 7; следовательно, и данное число не делится на 7.

Заметим, что при умножении всех однозначных цифр на однозначное число, взаимно-простое с 10 (т. е. на 1, 3, 7, 9), мы получаем каждый раз полную систему вычетов по модулю 10 (§ 32, пример 5), т. е. последние цифры в произведениях будут все цифры 0, 1, 2, ... 9, и каждая *по одному разу*. Это дает возможность при небольшом d с цифрою единиц 1, 3, 7 или 9 исследовать делимость числа N на d, деля «с конца». Например, при $N = 458346$, $d = 7$:

```
458346 | 7
    56 |-----
------ | 65478
  829  |
   49
  ---
   78
   28
  ---
   55
   35
  ---
   42
   42
  ---
```

Рассуждаем так: если данное число делится на 7, то последняя цифра частного непременно равна 8, ибо только произведение $7 \cdot 8$ имеет последнюю цифру 6. Отнимем от данного числа 56 и зачеркнем последний нуль; получим 45829. Здесь последняя цифра 9; следовательно, предпоследняя цифра частного равна 7, ибо только $7 \cdot 7$ имеет последнюю цифру 9, и т. д.

В нашем примере данное число делится на 7, так как в результате деления мы получили остаток равный 0. Конечно, при выяснении делимости числа на 7 нам не нужны цифры частного; надо только знать произведения $7 \cdot 2$, $7 \cdot 3$, $7 \cdot 4 \ldots$, а это известно из обычной таблицы умножения.

Рассуждаем так: число 458346 оканчивается цифрой 6; откинем эту цифру, а от 34 отнимем 5, получим 29; откинем 9, а от 82 отнимем 4, получим 78; откинем 8, а от 7 отнимем 2, получим 5; откинем 5, а от следующей слева цифры 5 отнимем 3, получим 42, а это делится на 7.

Вместо того чтобы отнимать, мы могли бы прибавлять дополнения до 7. Так, возьмем опять число 458346; отнимем 6, а к 4 прибавим 2, получим 45836; далее откинем 6, а к 3 прибавим 2; получим 4585; откинем 5, а к 8 прибавим 4, получим 462; откинем 2, а к 6 прибавим 3, получим 49, которое делится на 7.

По существу это только вариант (а иногда и упрощение) способа Жбиковского.

Пример. Найти, делится ли 42315 на 13.

Откинем 5, а от 31 отнимем 6, получим 25; опять откинем 5, а от 22 отнимем 6, получим 16; откинем 6, а от 41 отнимем 2, получим 39,— делится на 13.

Замечание. Оба изложенных общих способа можно применять не только для десятичной, но и для любой системы счисления (с любым основанием A). Конечно, признаки делимости на отдельные числа d будут тогда совсем иными (см. упражнения в конце этой главы).

§ 43. Система сравнений с разными модулями. Этот случай не имеет аналогии в теории уравнений. Общая задача следующая: даны несколько сравнений 1-й степени с одним и тем же неизвестным, но с разными модулями: $ax \equiv b \pmod{m}$, $a_1 x \equiv b_1 \pmod{m_1}$, ... Требуется определить число x, удовлетворяющее всем этим сравнениям.

Прежде всего заметим, что каждое из этих сравнений можно решить отдельно, заблаговременно, т. е. с самого начала взять сравнения в таком виде: $x \equiv c \pmod{m}$, $x \equiv c_1 \pmod{m_1}$, ..., так как если хоть одно из данных сравнений не имеет решения, то задача вообще невозможна.

Рассмотрим сначала случай двух сравнений:

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}. \tag{88}$$

Первое из этих сравнений дает: $x = c_1 + m_1 t$; подставляя это вместо x во второе сравнение (88), получим: $c_1 + m_1 t \equiv c_2 \pmod{m_2}$, или

$$m_1 t \equiv c_2 - c_1 \pmod{m_2}. \tag{89}$$

Это сравнение имеет решение t тогда и только тогда, когда $c_2 - c_1$ делится на $d = D(m_1, m_2)$ (теорема 60, § 39) и общее ре-

шение имеет вид: $t \equiv t_0 + \frac{m_2}{d} u$ (§ 39, (80)), где t_0 — какое-нибудь частное решение сравнения (89), а u — произвольное целое число.

Подставляя это значение t в формулу $x = c_1 + m_1 t$, получим: $x = c_1 + m_1 t_0 + \frac{m_1 m_2}{d} u$; но $\frac{m_1 m_2}{d} = M = \text{М}(m_1, m_2)$ (5, теорема 12). Обозначив еще $c_1 + mt_0 = x_0$, получим общее решение сравнений (88):

$$x \equiv x_0 \pmod M, \tag{90}$$

где x_0 — частное решение (при $u = 0$).

Итак:

Теорема 62. Система сравнений (88) имеет решения тогда и только тогда, когда $c_2 \equiv c_1 \pmod{D(m_1, m_2)}$; все решения сравнимы друг с другом по модулю $\text{М}(m_1, m_2)$. В частности, если m_1 и m_2 взаимно-простые, то система (88) всегда имеет решение,— единственное по модулю $m_1 m_2$.

Пример 1. $x \equiv 7 \pmod{33}$, $x \equiv 13 \pmod{63}$.

Здесь условие $7 \equiv 13 \pmod{D(33, 63)}$ выполнено, ибо $D(33, 63) = 3$. Первое сравнение дает: $x = 7 + 33t$; подставляя это во второе сравнение, получим: $33t \equiv 6 \pmod{63}$, или: $11t \equiv 2 \pmod{21}$. Можно взять $t_0 = 4$; тогда $x_0 = 7 + 33 \cdot 4 = 139$, и общее решение есть $x \equiv 139 \pmod{693}$, так как $\text{М}(33, 63) = 693$.

Обобщение. Если нам даны несколько сравнений вида (88), то мы сначала решим первые два из них, т. е. заменим эти два сравнения одним вида (90); далее возьмем это полученное сравнение и еще одно из данных и решим их, и т. д. С каждым таким шагом мы уменьшаем на одно число сравнений; в конце концов, получим одно сравнение вида (90), где M, как легко видеть, будет общим наименьшим кратным всех модулей. Конечно, если на одном из этих этапов окажется, что взятые два сравнения не имеют решений, то и вся задача невозможна. Важно, когда все данные модули попарно взаимно-простые; в этом случае система всегда имеет решение,— единственное по модулю, равному произведению всех данных модулей.

Пример 2. Дана система: $x \equiv 3 \pmod{11}$, $x \equiv -2 \pmod{13}$, $x \equiv 5 \pmod 7$.

Первые два сравнения дают: $x = 3 + 11t$; $11t \equiv -5 \pmod{13}$, или $2t \equiv -8$, $t \equiv -4 \pmod{13}$ и решение двух первых сравнений есть:

$$x \equiv 3 - 4 \cdot 11 = -41 \pmod{143}.$$

Теперь берем это решение и последнее из данных сравнений:

$$x \equiv -41 \pmod{143}, \quad x \equiv 5 \pmod 7;$$

это дает: $x = -41 + 143u$; $143u \equiv 46 \pmod 7$, или (приводя по модулю 7): $3u \equiv -3 \pmod 7$, $u \equiv -1$, следовательно: $x = -41 - 143 = -184$ и общее решение:

$$x \equiv -184 \pmod{1001}.$$

Приведем еще один способ решения такой системы сравнений, когда модули попарно взаимно-простые.

Пусть дана система сравнений:

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \ \dots \ x \equiv c_k \pmod{m_k}.$$

Пусть $x_1, \ x_2, \dots x_k$ решения следующих вспомогательных сравнений:

$$m_2 m_3 \dots m_k x_1 \equiv 1 \pmod{m_1};$$
$$m_1 m_3 \dots m_k x_2 \equiv 1 \pmod{m_2};$$
$$\dots\dots\dots\dots\dots$$
$$m_1 m_2 \dots m_{k-1} x_k \equiv 1 \pmod{m_k}.$$

В таком случае решение данной системы есть:

$$x \equiv m_2 m_3 \dots m_k x_1 c_1 + m_1 m_3 \dots m_k x_2 c_2 + \dots + m_1 m_2 \dots m_{k-1} x_k c_k \pmod{m_1 m_2 \dots m_k}.$$

Ибо очевидно, что определенное таким образом число x сравнимо с c_1 по модулю m_1 с c_2 по модулю m_2 и т. д.

Пример 3. Старая китайская задача: найти число, которое при делении на 3 дает остаток 2, при делении на 5 дает остаток 3, при делении на 7 дает остаток 2.

В нашей символике эта задача сводится к такой системе сравнений:

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

Мы имеем здесь такие вспомогательные сравнения:

$$35x_1 \equiv 1 \pmod 3, \quad 21x_2 \equiv 1 \pmod 5, \quad 15x_3 \equiv 1 \pmod 7;$$

это дает: $x_1 = 2, \ x_2 = 1, \ x_3 = 1$. Таким образом

$$x \equiv 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 140 + 63 + 30 = 233 \pmod{105},$$

или (приводя по модулю 105)

$$x \equiv 23 \pmod{105}.$$

§ 44. Сравнения высших степеней с простым модулем. Общий вид такого сравнения n-й степени есть:

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \equiv 0 \pmod p; \qquad (92)$$

p — простое число, a_0 — не делится на p, следовательно, существует такое число α, что $a_0 \alpha \equiv 1 \pmod p$ (§ 39, теорема 60).

Умножив (92) на α и заменив $a_0 \alpha$ единицей, получим:

$$x^n + b_1 x^{n-1} + \dots + b_{n-1} x + b_n \equiv 0 \pmod p. \qquad (92a)$$

Следовательно, можно всегда считать коэффициент высшего члена равным единице.

Обозначим левую часть сравнения (92) или (92a) через $f(x)$

и пусть сравнение $f(x) \equiv 0 \pmod{p}$ имеет корень $x \equiv x_1 \pmod{p}$. Делим $f(x)$ на $x - x_1$; по теореме Декарта имеем:

$$f(x) = (x - x_1)\,\varphi(x) + f(x_1); \tag{93}$$

но ведь $f(x_1) \equiv 0 \pmod{p}$, следовательно, написав (93), как сравнение по модулю p, получим:

$$f(x) \equiv (x - x_1)\,\varphi(x) \pmod{p}. \tag{94}$$

Говорят, что $f(x)$ *делится на* $x - x_1$, *по модулю* p. Очевидно, что и обратно: из сравнения (94) вытекает, что $f(x_1) \equiv 0 \pmod{p}$, т. е. x_1 — корень сравнения (92).

Итак:

Теорема 63. Сравнение (92) имеет корень $x \equiv x_1$ тогда и только тогда, когда левая его часть делится на $x - x_1$ по данному модулю p.

Заметим, что эта теорема верна и для составного модуля m.

Возьмем теперь сравнение $(n-1)$-й степени $\varphi(x) \equiv 0 \pmod{p}$, где $\varphi(x)$ — та же функция, что и в (94). Пусть это сравнение имеет корень $x \equiv x_2$; тогда мы так же выведем следующее тождественное сравнение:

$$\varphi(x) \equiv (x - x_2)\,\psi(x) \pmod{p}.$$

Подставляя отсюда значение $\varphi(x)$ в правую часть формулы (94), найдем:

$$f(x) \equiv (x - x_1)(x - x_2)\,\psi(x) \pmod{p}, \tag{95}$$

где $\psi(x)$ — целая рациональная функция $(n-2)$-й степени. (95) показывает, что $f(x_2) \equiv 0$, т. е., что x_2 — тоже корень сравнения (92); если $x_2 \equiv x_1 \pmod{p}$, то корень x — *кратный*. Обратно, если $x \equiv x_2$ — корень сравнения (92) и $x_2 \not\equiv x_1 \pmod{p}$, то x_2 непременно корень и сравнения $\varphi(x) \equiv 0 \pmod{p}$, так как тогда (94) дает:

$$(x_2 - x_1)\,\varphi(x_2) \equiv 0 \pmod{p}.$$

Следовательно, произведение $(x_2 - x_1)\,\varphi(x_2)$ делится на p; тогда (по теореме 19, § 10) по крайней мере один из сомножителей делится на p; но $x_2 - x_1$ не делится на p, значит, $\varphi(x_2) \equiv 0 \pmod{p}$.

Пусть и сравнение $\psi(x) \equiv 0 \pmod{p}$ имеет корень x_3; тогда подобно же выведем:

$$f(x) \equiv (x - x_1)(x - x_2)(x - x_3)\,\omega(x) \pmod{p},$$

где $\omega(x)$ — целая рациональная функция $(n-3)$-й степени, и т. д. Но здесь мы не всегда придем к разложению функции $f(x)$ n-й степени на n линейных множителей по модулю p, ибо здесь не действительна теорема о том, что всякое сравнение любой степени имеет корень. Таким образом, в конце концов мы придем к следующей формуле:

$$f(x) \equiv (x - x_1)(x - x_2)\,\ldots\,(x - x_k)\,g(x) \pmod{p}, \tag{96}$$

где $g(x)$ — целая рациональная функция $(n-k)$-й степени и сравнение $g(x) \equiv 0 \pmod{p}$ совсем не имеет корней (конечно, $n-k>1$). Данное же сравнение $f(x) \equiv 0 \pmod{p}$ имеет всего k корней: x_1, $x_2, \ldots x_k$; они не непременно все различны по модулю p. Но иных корней, кроме этих, сравнение $f(x) \equiv 0 \pmod{p}$ не может иметь, так как если x — какой-нибудь корень этого сравнения, то при этом значении x правая часть (96) делится на p, а следовательно, по крайней мере один из сомножителей этой части делится на p (§ 10, теорема 19). Но $g(x)$ не делится на p, так как сравнение $g(x) \equiv 0$ не имеет корней; следовательно, x сравнимо с каким-нибудь x_λ.

Заметим, что этот вывод правилен только для простого модуля p, ибо теорема 19 в § 10 верна только для простых делителей. В частности, может случиться, что в (96) $k=n$, т. е. что функция $f(x)$ n-й степени раскладывается по модулю p на n линейных множителей. В этом случае $g(x)$ — постоянная величина (не зависит от x), и легко видеть, что $g(x) \equiv a_0 \pmod{p}$, так как это— коэффициент при x^n в правой части (96), т. е. можно взять $g=a_0$, и мы имеем в этом случае:

$$f(x) \equiv a_0(x-x_1)(x-x_2) \ldots (x-x_n) \pmod{p}. \qquad (96a)$$

Это тождественное сравнение показывает, что сравнение (92) имеет в этом случае n корней: $x_1, x_2, \ldots x_n$, которые могут быть и не все различны по модулю p. Кроме этих корней сравнение (92) иных корней не может иметь.

Итак:

Теорема 64. Сравнение n-й степени по простому модулю p не может иметь больше, чем n корней, различных по модулю p. Если оно имеет n корней, то левая его часть раскладывается по модулю p на n линейных множителей.

Заметим, что для составного модуля эта теорема совсем неверна; например, сравнение 2-й степени:

$$x^2 \equiv 1 \pmod{8}$$

имеет четыре различных по модулю 8 корня: 1, 3, 5, 7.

Следствие. Сравнение n-й степени по простому модулю p, имеющее больше чем n различных по модулю p корней,— тождественное, т. е. все коэффициенты его левой части делятся на p.

Доказательство. Если наше сравнение n-й степени $f(x) \equiv \equiv 0 \pmod{p}$ имеет $n+1$ различных по модулю p корней: $x_1, x_2 \ldots \ldots x_n, x_{n+1}$, то (96a) дает

$$a_0(x_{n+1}-x_1)(x_{n+1}-x_2) \ldots (x_{n+1}-x_n) \equiv 0 \pmod{p}.$$

Но ни одна из разностей $x_{n+1}-x_\lambda$ не делится на p, так как $x_{n+1} \not\equiv x_\lambda$; следовательно, a_0 делится на p, т. е. $a_0 \equiv 0 \pmod{p}$, и данное сравнение не n-й, а более низкой степени. Если уже известно, что наше следствие верно для сравнений степени $<n$, то мы получили, что это следствие верно и для сравнений n-й

степени. Но для сравнений 1-й степени следствие верно, ибо если x_1 и x_2 различные (по модулю p) корни сравнения $ax + b \equiv 0 \pmod{p}$, то $ax_1 + b \equiv ax_2 + b$; $a(x_1 - x_2) \equiv 0$, т. е. $a \equiv 0 \pmod{p}$, а отсюда и $b \equiv 0 \pmod{p}$. Таким образом, наше следствие доказано методом полной индукции.

Частный случай. Рассмотрим сравнение

$$x^{p-1} - 1 \equiv 0 \pmod{p}. \qquad (97)$$

По теореме Ферма - Эйлера (§ 37, теорема 58) это сравнение имеет как раз $p-1$ различных корней $1, 2, 3, \ldots p-1$; следовательно, по теореме 64 мы имеем тождественное сравнение:

$$x^{p-1} - 1 \equiv (x-1)(x-2) \ldots (x-p+1) \pmod{p}.$$

Отсюда при $x = 0$ получим:

$$-1 \equiv (-1)(-2) \ldots (-p+1) \pmod{p},$$

или:

$$-1 \equiv (y-1)!(-1)^{p-1} \pmod{p}.$$

При $p > 2$ $p-1$ четное, следовательно,

$$(p-1)! \equiv -1 \pmod{p}.$$

Это — теорема Вильсона (§ 40, теорема 61 или формула (83)), которую мы, таким образом, еще раз доказали; это доказательство принадлежит Лагранжу.

Теорема 65. Если сравнение n-й степени $f(x) \equiv 0 \pmod{p}$ имеет n различных корней, и $f(x)$ по модулю p раскладывается на два множителя $\varphi(x)$ и $\psi(x)$ k-й и l-й степеней ($k + l = n$), т. е. тождественно $f(x) \equiv \varphi(x)\psi(x) \pmod{p}$, то сравнение $\varphi(x) \equiv 0 \pmod{p}$ имеет k различных корней, а сравнение $\psi(x) \equiv 0 \pmod{p}$ имеет l различных корней.

Доказательство. Каждый корень сравнения $f(x) \equiv 0$ является корнем одного из сравнений $\varphi(x) \equiv 0$, $\psi(x) \equiv 0$; если бы сравнение $\varphi(x) \equiv 0$ имело меньше чем k различных корней, то $\psi(x) \equiv 0$ имело бы больше чем l различных корней, так как общее число корней $= n = k + l$. Но это невозможно по теореме 64, следовательно, $\varphi(x) \equiv 0$ имеет точно k различных корней, а $\psi(x) \equiv 0$ имеет точно l различных корней. Иными словами, все корни сравнения $f(x) \equiv 0$ распределяются между сравнениями $\varphi(x) \equiv 0$ и $\psi(x) \equiv 0$.

Теорема 66. Сравнение n-й степени $f(x) \equiv 0 \pmod{p}$ при $n \geq p$ равносильно с некоторым сравнением степени меньшей чем p.

Доказательство. Умножив обе части сравнения (97) на x, получим сравнение:

$$x^p - x \equiv 0 \pmod{p}, \qquad (98)$$

имеющее p корней: $x \equiv 0, 1, 2, \ldots p-1$; т. е. это сравнение удовлетворяется всяким целым числом. Разделим функцию $f(x)$ на $x^p - x$:

$$f(x) \equiv (x^p - x)\varphi(x) + \psi(x) \pmod{p};$$

степень $\psi(x) < p$. Для всякого целого числа x в силу сравнения (98) имеем:

$$f(x) \equiv \psi(x) \pmod p,$$

следовательно, и корни сравнений $f(x) \equiv 0$ и $\psi(x) \equiv 0$ одни и те же, так как при $f(x_1) \equiv 0$ и $\psi(x_1) \equiv 0$, и обратно.

Замечание. Мы можем только утверждать, что сравнения $f(x) \equiv 0$ и $\psi(x) \equiv 0$ имеют одни и те же корни; но об их кратности теорема 66 ничего не говорит. Может случиться, что кратный корень сравнения $f(x) \equiv 0$ будет простым для $\psi(x) \equiv 0$, однако может быть и наоборот.

Пример. Дано сравнение:

$$f(x) = x^5 + x^4 + x^3 - x^2 - 2 \equiv 0 \pmod 5.$$

Делим $f(x)$ на $x^5 - x$ и получаем:

$$x^5 + x^4 + x^3 - x^2 - 2 = (x^5 - x) \cdot 1 + (x^4 + x^3 - x^2 + x - 2);$$

следовательно,

$$\psi(x) = x^4 + x^3 - x^2 + x - 2.$$

Корни данного сравнения: $x_1 \equiv 1$, $x_2 \equiv 2$, $x_3 \equiv 3$; они удовлетворяют и сравнению $\psi(x) \equiv 0 \pmod 5$. Но легко проверить, что

$$x^5 + x^4 + x^3 - x^2 - 2 \equiv (x-1)^2 (x-2)^2 (x-3) \pmod 5,$$

тогда как

$$x^4 + x^3 - x^2 + x - 2 \equiv (x-1)(x-2)(x-3)^2 \pmod 5,$$

т. е. для сравнения $f(x) \equiv 0$ корни 1 и 2 — двойные, а 3 — простой, а для сравнения $\psi(x) \equiv 0$ корни 1 и 2 простые, а 3 — двойной.

Следствие. Сравнение $f(x) \equiv 0 \pmod p$ тогда и только тогда удовлетворяется всяким целым значением x, когда $\psi(x) \equiv 0 \pmod p$ — тождественное сравнение, т. е. все коэффициенты функции $\psi(x)$ делятся на p (или иначе: когда $f(x)$ делится на $x^p - x$ без остатка по модулю p).

Доказательство. Ибо в этом случае сравнение $\psi(x) \equiv 0 \pmod p$ степени $< p$ имеет p различных корней (см. следствие из теоремы 63).

Замечание. В § 38 мы указывали, что существуют нетождественные сравнения, которым удовлетворяет всякое целое значение неизвестного. Теперь мы нашли и общий вид такого сравнения с одним неизвестным по простому модулю: это — сравнение $f(x) \equiv 0 \pmod p$, где $f(x)$ делится по модулю p на $x^p - x$ без остатка. Таким образом, в теории сравнений с простым модулем p функция $x^p - x$ играет особую роль.

Теорема 67. Сравнение $f(x) \equiv 0 \pmod p$ степени $n < p$ тогда и только тогда имеет n различных корней, когда все коэффициенты

остатка от деления $x^p - x$ на $f(x)$ делятся на p (иными словами, если $x^p - x$ делится по модулю p на $f(x)$ без остатка).

Доказательство. Пусть.

$$x^p - x \equiv f(x)\varphi(x) + \psi(x) \pmod p. \qquad (99)$$

1) Пусть сравнение $f(x) \equiv 0$ имеет n различных корней $x_1, x_2 \ldots \ldots x_n$; но ведь эти корни удовлетворяют и сравнению (98), следовательно, и сравнению $\psi(x) \equiv 0$, а значит (по следствию из теоремы 64) сравнение $\psi(x) \equiv 0$ тождественное, т. е. все коэффициенты функции $\psi(x)$ делятся на p.

2) Пусть теперь нам дано, что все коэффициенты в $\psi(x)$ делятся на p; в таком случае (99) дает: $x^p - x \equiv f(x)\varphi(x) \pmod p$, и мы по теореме 65 заключаем, что сравнение $f(x) \equiv 0$ имеет n различных корней.

УПРАЖНЕНИЯ

41. Образуют ли степени 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 вместе с числом 0 полную систему вычетов по модулю 11? (§ 32).

Ответ. Образуют.

42. Привести к простейшему виду функцию: $14x^5 - 25x^4 + 35x^3 + 15x^2 - 19x + 5$ по модулю 7 (§ 33).

Ответ. $3x^4 + x^2 + 2x - 2$.

43. Подставляя в выражение $z = 5y + 3x$ значения $x = 0$, 1, 2, 3, 4; $y = 0$, 1, 2, проверить, что мы получим для z полную систему вычетов по модулю 15 (§ 35, теорема 54).

44. Вычислить $\varphi(m)$ для $m = 1, 2, 3, \ldots 20$ (§ 35).

45. Проверить формулу Гаусса для $m = 30$ (§ 35, теорема 55).

46. Вычислить $\varphi(72)$, $\varphi(75)$, $\varphi(125)$, $\varphi(1001)$ (§ 35).

Ответ. 24, 40, 100, 720.

47. Найти $\mu(m)$ для $m = 1, 2, 3, \ldots, 20$ (§ 36).

48. По формуле Лиувилля - Дедекинда найти «числовую производную» $\Phi(m)$ для функции $F(m) = 1$ (для всякого m) (§ 36, формула (68)).

Ответ. $\Phi(1) = 1$; для $m > 1$ $\Phi(m) = 0$.

49. Проверить формулы: $5^{\varphi(24)} \equiv 1 \pmod{24}$, $2^{\varphi(33)} \equiv 1 \pmod{33}$, $3^{\varphi(20)} \equiv 1 \pmod{20}$ (возводя в степени по модулям) (§ 37).

50. Найти показатель, к которому принадлежит: а) 5 по модулю 12; б) 2 по модулю 25; в) 4 по модулю 33; г) 3 по модулю 28 (§ 37).

Ответ. а) 2; б) 20; в) 5; г) 6.

51. Решить сравнения: а) $7x \equiv 10 \pmod{18}$; б) $25x \equiv 1 \pmod{17}$; в) $13x \equiv 32 \pmod{28}$; г) $132x \equiv 11 \pmod{59}$ (§ 39).

Ответ: а) 4; б) —2; в) —4; г) 5.

52. Решить сравнения: а) $28x \equiv 21 \pmod{35}$; б) $38x \equiv 4 \pmod{26}$; в) $112x \equiv 45 \pmod{119}$; г) $36x \equiv 54 \pmod{18}$; д) $286x \equiv 121 \pmod{341}$ (§ 39).

Ответ. а) 2, 7, 12, 17, 22, 27, 32; б) —4, 9; в) решений нет; г) сравнение тождественное; д) 4, 35, 66, 97, 128, 159, 190, 221, 252, 283, 314.

53. Если $ax \equiv b \pmod{m}$ и $D(a, m) = 1$, то решение (единственное) этого сравнения символически обозначится как дробь: $x \equiv \frac{b}{a} \pmod{m}$.

Найти: $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, $\frac{1}{6} \pmod{7}$ (§ 39).

Ответ. 4, 5, 2, 3, 6.

54. Найти $\frac{1}{47} \pmod{93}$, $\frac{23}{37} \pmod{50}$, $\frac{49}{102} \pmod{121}$ (обозначение как в задаче 53) (§ 39).

Ответ. 2; 29; 42.

55. Доказать, что $\frac{b}{a} \equiv \frac{bk}{ak} \pmod{m}$, если и a и k — взаимно-простые с m (обозначение как в задаче 53).

56. Вывести формулу: $\frac{b_1}{a_1} \pm \frac{b_2}{a_2} \equiv \frac{a_2b_1 \pm a_1b_2}{a_1a_2} \pmod{m}$ (обозначение как в задаче 53; a_1, a_2 взаимно-простые с m).

57. Вывести формулу: $\frac{b_1}{a_1} \cdot \frac{b_2}{a_2} \equiv \frac{b_1b_2}{a_1a_2} \pmod{m}$ (дроби — символические, как в задаче 53; a_1, a_2 — взаимно-простые с m).

58. Вывести формулу: $\frac{b_1}{a_1} : \frac{b_2}{a_2} \equiv \frac{b_1a_2}{a_1b_2} \pmod{m}$. Здесь $\frac{b_1}{a_1} : \frac{b_2}{a_2}$ — корень сравнения $\frac{b_2}{a_2} x \equiv \frac{b_1}{a_1} \pmod{m}$; дроби — символические, по модулю m; a_1, a_2, b_2 — взаимно-простые с m.

59. Проверить теорему Вильсона при $p = 5$ и $p = 7$ (§ 40).

60. Найти число цифр в периоде десятичных дробей, в которые обращаются обыкновенные дроби со знаменателями: 3, 7, 11, 17, 19, 21 (§ 41).

Ответ. 1, 6, 2, 16, 18, 6.

61. Обратить следующие периодические дроби в обыкновенные: 0,35(62); 5,1(538); 3,(27); 11,12(31) (§ 41).

Ответ. $\frac{3527}{9900}$; $\frac{51487}{9990}$; $\frac{36}{11}$; $\frac{110119}{9900}$.

62. Разложить на простые множители числа: 2717, 7567, 1813, 9971, 1309 (§ 42).

Ответ. $11 \cdot 13 \cdot 19$; $7 \cdot 23 \cdot 47$; $7^2 \cdot 37$; $13^2 \cdot 59$; $7 \cdot 11 \cdot 17$.

63. Найти признаки делимости на 2, 3, 4, 5, 7, 9 для восьмиричной системы счисления (т. е. для системы с основанием 8) (§ 42).

Ответ. На 2 делится число, оканчивающееся четной цифрой (включая и 0); на 3 и на 9 делится число, для которого разность между суммой цифр, стоящих на четных местах, и суммой цифр, стоящих на нечетных местах, делится на 3 или на 9; на 4 делится число, оканчивающееся нулем или цифрой 4; на 5 делится число $a_0 + 8a_1 + 8^2a_2 + 8^3a_3 + \ldots$, если выражение $a_0 - 2a_1 - a_2 + 2a_3 + a_4 - 2a_5 - a_6 + \ldots$ делится на 5; на 7 делится число, сумма цифр которого делится на 7.

64. Найти признаки делимости на 2, 3, 4, 5, 6, 7, 8, 9, 11, 13 для двенадцатиричной системы счисления (§ 42).

Ответ. На 2 делится число, оканчивающееся четной цифрой (включая и 0); на 3 делится число, оканчивающееся цифрой 0, 3, 6 или 9; на 4 делится число, оканчивающееся цифрой 0, 4 или 8; на 5 делится число $a_0 + 12a_1 + 12^2a_2 + \dots$, если число $a_0 + 2a_1 - a_2 - 2a_3 + a_4 + 2a_5 - \dots$ делится на 5; на 6 делится число, оканчивающееся нулем или цифрой 6; на 7 делится число $a_0 + 12a_1 + 12^2a_2 + \dots$, если число $a_0 - 2a_1 - 3a_2 - a_3 + 2a_4 + 3a_5 + a_6 - 2a_7 - 3a_8 + \dots$ делится на 7; на 8 делится число $a_0 + 12a_1 + 12^2a_2 + \dots$, если число $a_0 + 4a_1$ делится на 8; на 9 делится то же число, если число $a_0 + 3a_1$ делится на 9; на 11 делится число, сумма цифр которого делится на 11; на 13 признак делимости тот же, что в десятичной системе на 11.

65. Решить систему сравнений: а) $x \equiv 1 \pmod 7$, $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 9$; б) $x \equiv 5 \pmod{48}$, $x \equiv 17 \pmod{36}$; в) $x \equiv 1 \pmod{25}$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 7$, $x \equiv 4 \pmod 9$ (§ 43).

Ответ. а) $x \equiv 113 \pmod{315}$; б) $x \equiv 53 \pmod{144}$; в) $x \equiv 4126 \pmod{6300}$.

66. Решить систему сравнений: а) $3x \equiv 5 \pmod 4$, $5x \equiv 2 \pmod 7$; б) $4x \equiv 3 \pmod{25}$, $3x \equiv 8 \pmod{20}$; в) $x \equiv 8 \pmod{15}$, $x \equiv 5 \pmod{18}$, $x \equiv 13 \pmod{25}$ (§ 43).

Ответ. а) $x \equiv -1 \pmod{28}$; б) решений нет; в) $x \equiv 113 \pmod{450}$.

67. Разложить на множители по модулю 7 следующие функции (найдя пробами их корни по модулю 7): а) $3x^4 + x^2 + 5x - 2$; б) $2x^3 + 5x^2 - 2x - 3$; в) $x^4 - 2x^2 + x + 1$ (§ 44).

Ответ. а) $(x-1)(3x^3 + 2x^2 - 3x + 2)$; б) неприводима; в) $(x - 2)(x - 3)(x^2 - 2x + 3)$.

68. Разложить на множители по модулю 11 следующие функции: а) $2x^4 + x^3 - 3x^2 - 2x - 2$; б) $x^4 + x + 4$ (§ 44).

Ответ. а) $2(x - 2)(x - 3)(x^2 - 2)$; б) $(x - 2)^2(x - 3)(x - 4)$.

69. Привести сравнения: а) $x^7 - 6 \equiv 0 \pmod 5$; б) $x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \pmod 5$ к сравнениям степеней <5 (§ 44).

Ответ. а) $x^3 \equiv 1 \pmod 5$; б) $2x^3 + 3 \equiv 0 \pmod 5$.

70. Применяя теорему 67 (§ 44), найти, имеют ли сравнения $x^2 + 2x - 1 \equiv 0 \pmod 7$, $x^3 + x - 3 \equiv 0 \pmod 7$ — первое два различных корня, второе — три различных корня.

Ответ. Первое имеет, второе — нет.

ГЛАВА IV

КВАДРАТИЧНЫЕ ВЫЧЕТЫ

§ 45. Сравнения по сложному модулю. Теорема 68. Если $m = m_1 m_2 \ldots m_k$, где все m_λ попарно взаимно-простые, то сравнение:

$$f(x) \equiv 0 \pmod{m} \qquad (100)$$

эквивалентно системе сравнений:

$$f(x) \equiv 0 \pmod{m_1}, \; f(x) \equiv 0 \pmod{m_2}, \; \ldots \; f(x) \equiv 0 \pmod{m_k} \qquad (101)$$

и число решений (по модулю m) сравнения (100) равно произведению чисел решений сравнений (101) (каждое из решений — по соответствующему модулю).

Доказательство. Всякое решение сравнения (100) удовлетворяет каждому из сравнений (101) (по теореме 45, § 33). Обратно, если x_0 — общее решение сравнений (101), то x_0 удовлетворяет и сравнению (100) (по теореме 46, § 33 и теореме 17, § 8). Пусть, далее, x_1 — корень первого сравнения (101), x_2 — корень второго сравнения (101) и т. д. В таком случае всегда можно найти число x_0 (§ 43, обобщение теоремы 62) так, чтобы было:

$$x_0 \equiv x_1 \pmod{m_1}, \; x_0 \equiv x_2 \pmod{m_2}, \; \ldots \; x_0 \equiv x_k \pmod{m_k}.$$

Число x_0 определяется по модулю m; оно является общим корнем всех сравнений (101), а следовательно, и сравнения (100). Этим доказывается и последняя часть теоремы 68.

Следствие 1. Если хоть одно из сравнений (101) не имеет решений, то и сравнение (100) тоже не имеет решений.

Следствие 2. Решения сравнений с каким-нибудь модулем m сводятся к решениям сравнений, модули которых — степени простых чисел.

Доказательство. Ибо $m = p^\alpha q^\beta r^\gamma \ldots$, где $p, q, r, \ldots$ различные простые делители числа m, и $p^\alpha, q^\beta, r^\gamma, \ldots$ попарно взаимно-простые.

§ 46. Квадратные сравнения. Общий вид такого сравнения:

$$ax^2 + bx + c \equiv 0 \pmod{m}. \qquad (102)$$

Это сравнение эквивалентно такому:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am} \qquad (102а)$$

(§ 33, теорема 47 и следствие 1 из теоремы 50). Сравнение (102а) можно легко преобразовать к виду

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}$$

или, обозначив $D = b^2 - 4ac$, $y = 2ax + b$,

$$y^2 \equiv D \pmod{4am}. \qquad (103)$$

Обратно, если мы нашли решение y сравнения (103), то для решения x сравнения (102) имеем: $x = \frac{y-b}{2a}$; если $y - b$ делится на $2a$ (что́ не всегда бывает), то получаем решение x сравнения (102). Таким образом, среди решений y сравнения (103) бывают такие, которым соответствуют решения x сравнения (102). Однако могут быть и такие, которым не соответствуют решения x; может случиться, что различным по модулю $4am$ решениям y соответствуют решения x, не различные по модулю m. Но, исследуя таким образом все решения сравнения (103), мы наверно найдем все решения x сравнения (102), ибо каждому решению сравнения (102) непременно соответствует решение y сравнения (103). Если (103) совсем не имеет решений, то и (102) тоже не имеет решений.

Таким образом:

Теорема 69. Квадратное сравнение общего вида (102) всегда можно привести к двучленному сравнению вида (103).

Укажем два случая, когда приведение сравнения (102) к двучленному упрощается.

1. Пусть a взаимно-простое с m; тогда можно найти α из сравнения $a\alpha \equiv 1 \pmod{m}$ (§ 39, теорема 60); умножив на α обе части сравнения (102) и заменив $a\alpha$ единицей, получим:

$$x^2 + b_1x + c_1 \equiv 0 \pmod{m}. \qquad (102б)$$

Умножив обе части и модуль на 4 и обозначив $2x + b_1 = y$, получим сравнение для y:

$$y^2 \equiv D \pmod{4m}, \qquad (103а)$$

где $D = b_1^2 - 4c_1$. Здесь мы можем утверждать, что каждое решение y сравнения (103а) непременно дает и решение x сравнения (102б) (только различным y по модулю $4m$ могут соответствовать одинаковые x по модулю m), ибо $x = \frac{y - b_1}{2}$, а $y - b_1$ всегда четное, как видно из (103а): $y^2 - b_1^2 \equiv -4c_1 \pmod{4m}$.

2. Пусть $b = 2l$ — четное число; тогда имеем сравнение:

$$ax^2 + 2lx + c \equiv 0 \pmod{m}. \qquad (102в)$$

Чтобы свести его к двучленному, достаточно умножить все три его части только на a и обозначить: $ax + l = y$. Получим для y:

$$y^2 \equiv D \pmod{am}, \qquad (103б)$$

где $D = l^2 - ac$. Этот случай имеет место всегда, если модуль m нечетный, так как тогда, если b — нечетное, можно заменить b через $b + m$ — четное число.

Конечно, оба эти случая могут быть одновременно: b — четное и a взаимно-простое с m; наше сравнение в этом случае:

$$x^2 + 2lx + c \equiv 0 \pmod{m}.$$

Обозначим: $x + l = y$; получим для y:

$$y^2 \equiv D \pmod{m},$$

где $D = l^2 - c$. Этот случай представляется, например, тогда, когда модуль $m = p$ — нечетное простое число.

Итак, из теорем 68 и 69 следует:

Следствие. Всякое квадратное сравнение сводится к системе сравнений вида

$$x^2 \equiv a \pmod{p^\alpha}, \tag{104}$$

где p — простое число.

В дальнейшем мы рассмотрим следующие случаи сравнения (104):

I. Сравнение (104) при p простом, нечетном и $\alpha = 1$;

II. Сравнение (104) при p простом, нечетном и при любом целом $\alpha > 1$.

III. Сравнение (104) при $p = 2$.

§ 47. Итак, переходим к исследованию сравнения:

$$x^2 \equiv a \pmod{p}, \tag{104a}$$

где p — простое нечетное число.

Теорема 70. Если $a \equiv 0 \pmod{p}$, то сравнение (104а) имеет только одно решение: $x \equiv 0 \pmod{p}$.

Доказательство. При $a \equiv 0$ имеем $x^2 \equiv 0 \pmod{p}$, а отсюда по теореме 19 (§ 10) имеем: $x \equiv 0 \pmod{p}$.

Теорема 71 (критерий Эйлера). Если a не делится на p (а следовательно, взаимно-простое с p), то сравнение (104а) имеет или два решения, или не имеет ни одного,— в зависимости от того, будет ли

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{105}$$

или:

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{105a}$$

Доказательство. Докажем сначала, что a непременно удовлетворяет одному и только одному из сравнений (105) и (105а). Именно, по теореме Ферма - Эйлера (§ 37, теорема 58)

$$a^{p-1} \equiv 1 \pmod{p};$$

отсюда:

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

По теореме 19 (§ 10) отсюда следует, что по крайней мере один из сомножителей $a^{\frac{p-1}{2}}-1$ или $a^{\frac{p-1}{2}}+1$ делится на p. Оба одновременно не могут делиться на p, так как их разность $=\pm 2$ не делится на нечетное число p. Следовательно, a удовлетворяет одному и только одному сравнению (105), (105a).

Пусть сравнение (104a) имеет решение x; тогда и $-x$ или $p-x$ — тоже решение, ибо $(-x)^2=x^2\equiv a \pmod p$. Эти два решения различны по модулю p: x, очевидно, не делится на p (ибо x^2-a делится на p). Если бы было $x\equiv -x \pmod p$, то мы имели бы: $2x\equiv 0 \pmod p$, а этого не может быть, так как ни 2, ни x не делятся на p (§ 10, теорема 19). Больше двух решений сравнение 2-й степени с простым модулем не может иметь (§ 44, теорема 64).

Возведя обе части сравнения (104a) в $\left(\frac{p-1}{2}\right)$-ю степень, получим (§ 33, следствие из теоремы 49):

$$x^{p-1}\equiv a^{\frac{p-1}{2}} \pmod p.$$

Но по теореме Ферма - Эйлера $x^{p-1}\equiv 1 \pmod p$, следовательно, если сравнение (104a) имеет корни, то a непременно удовлетворяет сравнению (105).

С другой стороны, если найти квадраты чисел $1, 2, 3, \ldots p-1$, то среди этих квадратов будут только $\frac{p-1}{2}$ чисел, различных по модулю p, так как числа α и $p-\alpha\equiv-\alpha$ дают одинаковые (по модулю p) квадраты, и кроме этих двух чисел ни одно из чисел $1, 2, \ldots p-1$ не даст такой же квадрат (иначе сравнение (104a) имело бы больше двух различных корней). Обозначим эти различные по модулю p квадраты чисел $1, 2, \ldots p-1$ так:

$$a_1,\ a_2,\ \ldots\ a_{\frac{p-1}{2}}. \tag{106}$$

Если a равно одному из чисел (106), то сравнение (104a) имеет решение, следовательно, все числа (106) удовлетворяют сравнению (105). Но сравнение (105) не может иметь больше чем $\frac{p-1}{2}$ различных (по модулю p) решений, следовательно, оно имеет как раз $\frac{p-1}{2}$ различных решений, и при a, равном любому из них, сравнение (104a) имеет решения. Отсюда же следует, что и сравнение (105a) имеет тоже $\frac{p-1}{2}$ различных (по модулю p) решений, и при a, равном любому из этих решений, сравнение (104a) не имеет решений. Этим теорема 71 доказана.

Определение. Если сравнение (104a) имеет решения, то a называется *квадратичным вычетом* числа p; в противном случае a называется *квадратичным невычетом* числа p *).

*) Иногда пропускают слово «квадратичный» и говорят просто «вычет» и «невычет».

Из доказательства теоремы 71 получается:

Следствие. Для нечетного простого p число его квадратичных вычетов всегда равно числу его квадратичных невычетов, а именно: $\frac{p-1}{2}$.

Теорема 72 (теорема Эйлера). Произведение двух квадратичных вычетов или двух невычетов есть вычет; произведение же вычета на невычет есть невычет.

Доказательство. Это непосредственно следует из критерия Эйлера: если a и b не делятся на p, то:

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p, \quad b^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Перемножив эти сравнения, найдем:

$$(ab)^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Здесь в правой части будет знак $+$, если в правых частях обоих предыдущих сравнений — одинаковые знаки, и знак $-$, если в предыдущих сравнениях разные знаки.

§ 48. Символ Лежандра. Если p — простое нечетное число и a не делится на p, то символ $\left(\frac{a}{p}\right)$ означает $+1$, если a — квадратичный вычет числа p, и -1, если a — квадратичный невычет числа p; этот символ ввел Лежандр (Legendre). Таким образом, вместо (105) и (105а) можно написать:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p. \tag{105б}$$

Мы выведем ряд свойств символа Лежандра, которые дадут возможность быстро вычислять его, а следовательно, определять, является ли a квадратичным вычетом или невычетом числа p, т е. имеет ли решение сравнение (104а) или не имеет. На этот вопрос дает ответ и критерий Эйлера, но если p — велико, то возводить a в $\left(\frac{p-1}{2}\right)$-ю степень весьма неудобно, тогда как вычислить символ Лежандра, как мы увидим дальше, весьма просто.

Свойства символа Лежандра.

I. Если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Это следует из общего закона, что в сравнениях можно каждое число заменить любым сравнимым с ним по данному модулю числом (§ 33).

II. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; это непосредственно обобщается на несколько сомножителей, в частности:

$$\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n; \quad \left(\frac{a^2}{p}\right) = +1; \quad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

Это свойство — просто символическое выражение теоремы Эйлера (теорема 72).

III. $\left(\frac{1}{p}\right) = +1$, ибо $1^{\frac{p-1}{2}} = 1$, т. е. единица — квадратичный вычет для всякого p.

IV. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$; критерий Эйлера здесь дает: $\left(\frac{-1}{p}\right) \equiv$ $\equiv (-1)^{\frac{p-1}{2}} \pmod p$. Но так как каждая часть этого сравнения равна ± 1, а $p > 2$, то обе части сравнения должны быть равны.

Это свойство словесно выражается так: -1 квадратичный вычет всех простых чисел вида $4k+1$ и квадратичный невычет всех простых чисел вида $4k+3$ (или $4k-1$). Ибо при $p = 4k+1$ показатель $\frac{p-1}{2} = 2k$ — четный, а при $p = 4k+3$ показатель $\frac{p-1}{2} =$ $= 2k+1$ — нечетный.

Свойство II сводит вычисление символа Лежандра $\left(\frac{a}{p}\right)$ при любом целом a к вычислению следующих символов Лежандра: $\left(\frac{1}{p}\right)$, $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$ (при нечетном простом $q \neq p$). Свойства III и IV дают формулы для $\left(\frac{1}{p}\right)$ и $\left(\frac{-1}{p}\right)$. Для $\left(\frac{2}{p}\right)$ имеется такая формула:

V. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ (мы докажем эту формулу в следующем параграфе).

По модулю 8 p имеет одну из таких форм: $8k+1$, $8k+3$, $8k+5$ (или $8k-3$), $8k+7$ (или $8k-1$). Если $p = 8k \pm 1$, то $\frac{p^2-1}{8} = 8k^2 \pm 2k$ — четное, следовательно, $(-1)^{\frac{p^2-1}{8}} = +1$. Если же $p = 8k \pm 3$, то $\frac{p^2-1}{8} = 8k^2 \pm 6k + 1$ нечетное; следовательно, $(-1)^{\frac{p^2-1}{8}} = -1$. Таким образом, свойство V словами выражается так: 2 — квадратичный вычет всех простых чисел вида $8k+1$ и $8k+7$ (или $8k-1$) и квадратичный невычет всех простых чисел вида $8k+3$ и $8k+5$ (или $8k-3$).

Что касается символов $\left(\frac{q}{p}\right)$, где p и q различные нечетные простые числа, то существует формула, которая связывает символы $\left(\frac{q}{p}\right)$ и $\left(\frac{p}{q}\right)$ и известна под именем *закона взаимности*. Существует много доказательств этого закона; мы дадим доказательство, основанное на следующей теореме:

Теорема 73 (лемма Гаусса). Если a не делится на простое нечетное число p, то

$$\left(\frac{a}{p}\right) = (-1)^{\mu}, \tag{107}$$

где μ — число отрицательных вычетов в ряде абсолютно-наименьших вычетов произведений $1a, 2a, \ldots \frac{p-1}{2}a$ по модулю p.

Доказательство. Обозначим через:

$$a_1, a_2, \ldots a_\lambda, -b_1, -b_2, \ldots -b_\mu \tag{108}$$

абсолютно-наименьшие вычеты чисел $a, 2a, \ldots \frac{p-1}{2}a$ по модулю p. Мы считаем все a_x и все b_y положительными, так что из чисел (108) λ положительных, μ — отрицательных, и $\lambda+\mu=\frac{p-1}{2}$; кроме того, все $a_x<\frac{p}{2}$ и все $b_y<\frac{p}{2}$. Числа (108) не сравнимы друг с другом по модулю p, так как и числа $a, 2a, \ldots \frac{p-1}{2}a$ не сравнимы: из $ka\equiv la \pmod p$ следует (§ 33, теорема 50, следствие 2), что $k\equiv l \pmod p$, а это возможно только при $k=l$, ибо и k и $l<\frac{p}{2}$. Но и числа a_x и b_y не сравнимы друг с другом по модулю p: именно, пусть $a_x\equiv b_y \pmod p$; но ведь $a_x\equiv ka \pmod p$, $-b_y\equiv la \pmod p$, следовательно, $ka\equiv -la \pmod p$, $ka+la=(k+l)a\equiv 0 \pmod p$, а значит $k+l\equiv 0 \pmod p$, чего не может быть, так как k и l положительные и меньшие чем $\frac{p}{2}$; следовательно, $k+l<p$ и положительно, потому и не может делиться на p. Таким образом, числа

$$a_1, a_2, \ldots a_\lambda, b_1, b_2, \ldots b_\mu \tag{108a}$$

все целые, положительные, различные по модулю p и каждое из них $<\frac{p}{2}$; их число: $\lambda+\mu=\frac{p-1}{2}$. Но ведь всего только и имеется $\frac{p-1}{2}$ целых положительных чисел, меньших чем $\frac{p}{2}$, а именно: $1, 2, 3, \ldots \frac{p-1}{2}$. Следовательно, числа (108a) и есть все числа $1, 2, 3, \ldots \frac{p-1}{2}$, только, может быть, расположены они в другом порядке; их произведение:

$$a_1a_2\ldots a_\lambda b_1b_2\ldots b_\mu=\left(\frac{p-1}{2}\right)! \tag{109}$$

Каждое из чисел (108) сравнимо с одним и только с одним произведением $ka\left(1\leq k\leq\frac{p-1}{2}\right)$ и обратно. Написав все эти сравнения и перемножив их, получаем, принимая во внимание (109):

$$\left(\frac{p-1}{2}\right)!\ a^{\frac{p-1}{2}}\equiv\left(\frac{p-1}{2}\right)!\ (-1)^\mu \pmod p;$$

сократив обе части на множитель $\left(\frac{p-1}{2}\right)!$, взаимно-простой с p,

получим:

$$a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod p.$$

Отсюда и из формулы (105б) получаем: $\left(\frac{a}{p}\right) = (-1)^{\mu}$, что и требовалось доказать.

§ 49. Закон взаимности. Так называется следующая теорема:

Теорема 74. Если p и q — два различных нечетных простых числа, то:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{110}$$

Мы уже знаем, что $\frac{p-1}{2}$ — четное или нечетное, в зависимости от того, что число p вида $4k+1$ или $4k+3$; то же самое и относительно $\frac{q-1}{2}$. Произведение $\frac{p-1}{2}\cdot\frac{q-1}{2}$ четное, если хоть один из сомножителей четный. Таким образом, закон взаимности можно выразить так:

Если хоть одно из чисел p, q вида $4k+1$, то

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right);$$

если же p, q оба вида $4k+3$, то

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Доказательство закона взаимности. Пусть a — целое число, не делящееся на p; делим a, $2a$, ... $\frac{p-1}{2}a$ на p:

$$\left.\begin{aligned} a &= q_1p + r_1 \\ 2a &= q_2p + r_2 \\ &\dots\dots\dots \\ xa &= q_xp + r_x \\ &\dots\dots\dots \\ \tfrac{p-1}{2}a &= q_{\frac{p-1}{2}}p + r_{\frac{p-1}{2}} \end{aligned}\right\} \tag{111}$$

Здесь $0 < r_x < p$; r_x — наименьшие положительные вычеты; беря те же обозначения, что и при доказательстве леммы Гаусса, можно убедиться, что числа r_1, r_2, ... $r_{\frac{p-1}{2}}$ те же самые, что и

$$a_1,\ a_2,\ \dots\ a_\lambda,\ p-b_1,\ p-b_2,\ \dots\ p-b_\mu;$$

следовательно:

$$\sum_{x=1}^{\frac{p-1}{2}} r_x = A - B + \mu p,$$

где обозначено:

$$a_1 + a_2 + \ldots + a_\lambda = A; \; b_1 + b_2 + \ldots + b_\mu = B.$$

Заметим еще, что:

$$1 + 2 + \ldots + \frac{p-1}{2} = \left(1 + \frac{p-1}{2}\right)\frac{p-1}{4} = \frac{p^2-1}{8}.$$

Теперь сложим почленно все равенства (111)

$$\frac{p^2-1}{8} \cdot a = p \sum_{x=1}^{\frac{p-1}{2}} q_x + \mu p + A - B. \qquad (112)$$

Но ведь числа $a_1, a_2, \ldots a_\lambda, b_1, b_2, \ldots b_\mu$ — это все числа $1, 2, \ldots \frac{p-1}{2}$ (см. доказательство леммы Гаусса), значит, их сумма:

$$A + B = \frac{p^2-1}{8}; \; A = \frac{p^2-1}{8} - B.$$

Следовательно, (112) дает $\left(\text{если перенести } \frac{p^2-1}{8} \text{ в левую часть}\right)$:

$$\frac{p^2-1}{8}(a-1) = p \sum_{x=1}^{\frac{p-1}{2}} q_x + \mu p - 2B. \qquad (112a)$$

1. Пусть $a = 2$; написав (112а), как сравнение по модулю 2, получим (приняв во внимание, что $p \equiv 1 \pmod 2$):

$$\frac{p^2-1}{8} \equiv \sum_{x=1}^{\frac{p-1}{2}} q_x + \mu \pmod 2.$$

Но в этом случае все $q_x = 0$, так как $1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots \frac{p-1}{2} \cdot 2$ все $< p$, т. е. при делении на p дают частные $=0$. Таким образом:

$$\frac{p^2-1}{8} \equiv \mu \pmod 2,$$

а отсюда по лемме Гаусса:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Таким образом, свойство V символа Лежандра (см. предыдущий параграф) доказано.

2. Пусть теперь $a = q$ — нечетное простое число, отличное от p; тогда (112а) дает, как сравнение по модулю 2:

$$0 \equiv \sum_{x=1}^{\frac{p-1}{2}} q_x + \mu \pmod 2,$$

или:

$$\sum_{x=1}^{\frac{p-1}{2}} q_x \equiv \mu \pmod 2.$$

Но q_x — неполное частное от деления xq на p, т. е. $q_x = \left[\frac{xq}{p}\right]$, следовательно:

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{xq}{p}\right] \equiv \mu \pmod 2.$$

Отсюда по лемме Гаусса получаем:

$$\left(\frac{q}{p}\right) = (-1)^{\sum \left[\frac{xq}{p}\right]}$$

аналогично найдем:

$$\left(\frac{p}{q}\right) = (-1)^{\sum \left[\frac{yp}{q}\right]}$$

и, следовательно,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum \left[\frac{xq}{p}\right] + \sum \left[\frac{yp}{q}\right]}$$

Нам нужно вычислить сумму:

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{xq}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{yp}{q}\right];$$

для этого рассмотрим выражение:

$$\frac{y}{q} - \frac{x}{p}, \tag{113}$$

где $x = 1, 2, \ldots \frac{p-1}{2}$; $y = 1, 2, \ldots \frac{q-1}{2}$. Таким образом всего у нас $\frac{p-1}{2} \cdot \frac{q-1}{2}$ значений разности (113); ни одна из них не равна нулю. Определим, сколько из них положительных и сколько отрицательных.

Пусть $\frac{y}{q} - \frac{x}{p} > 0$, т. е. $x < \frac{yp}{q}$; при данном y, x может иметь значения $1, 2, 3, \ldots \left[\frac{yp}{q}\right]$; а y имеет значения от 1 до $\frac{q-1}{2}$ включительно. Следовательно, существует всего $\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{yp}{q}\right]$ положительных

значений выражения (113). Пусть теперь $\frac{y}{q}-\frac{x}{p}<0$; тогда $y<\frac{xq}{p}$, и мы так же найдем, что имеется всего $\sum_{x=1}^{\frac{p-1}{2}}\left[\frac{xq}{p}\right]$ отрицательных значений выражения (113). А так как выражение (113) имеет всего $\frac{p-1}{2}\cdot\frac{q-1}{2}$ значений, каждое из которых непременно или положительно или отрицательно, то

$$\sum_{x=1}^{\frac{p-1}{2}}\left[\frac{xq}{p}\right]+\sum_{y=1}^{\frac{q-1}{2}}\left[\frac{yp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Отсюда непосредственно следует формула (110), т. е. закон взаимности доказан.

Закон взаимности первый открыл Эйлер в 1783 году, но не доказал его; снова нашел этот закон Лежандр в 1785 году, но доказательство, данное Лежандром, было неудовлетворительно. В 1798 году Лежандр выразил закон взаимности формулой (110) при помощи введенного им символа. Первый строго доказал закон взаимности Гаусс в 1796 году; это доказательство методом полной индукции помещено в знаменитой монографии Гаусса «Disquisitiones arithmeticae» («Арифметические исследования»), изданной в 1801 году. В дальнейшем Гаусс дал еще шесть доказательств закона взаимности. Доказательство, приведенное нами,— третье доказательство Гаусса с кое-какими упрощениями; последняя его часть принадлежит Кро́некеру (Kronecker). После Гаусса было дано еще много доказательств закона взаимности; в настоящее время их насчитывается около 50.

Закон взаимности вместе с другими свойствами символа Лежандра дает возможность вычислять этот символ, как мы покажем на примерах.

Пример 1. Вычислить $\left(\frac{438}{593}\right)$. Сначала разложим числитель 438 на простые множители:

$$438=2\cdot 3\cdot 73;$$

далее имеем по II, § 48:

$$\left(\frac{438}{593}\right)=\left(\frac{2}{593}\right)\left(\frac{3}{593}\right)\left(\frac{73}{593}\right).$$

Вычислим отдельно каждый символ правой части:

$$\left(\frac{2}{593}\right)=+1,$$

ибо по V, § 48, $593 = 8 \cdot 74 + 1$. Для вычисления $\left(\frac{3}{593}\right)$ сначала применим закон взаимности, а затем I, § 48:

$$\left(\frac{3}{593}\right) = \left(\frac{593}{3}\right) = \left(\frac{2}{3}\right).$$

Здесь мы перевернули символ Лежандра без перемены знака, ибо 593 вида $4k + 1$. Далее:

$\left(\frac{2}{3}\right) = -1$, ибо 3 вида $8k + 3$ (V, § 48). Следовательно,

$$\left(\frac{3}{593}\right) = -1.$$

Далее (по закону взаимности и по I и II § 48):

$$\left(\frac{73}{593}\right) = \left(\frac{593}{73}\right) = \left(\frac{9}{73}\right) = \left(\frac{3^2}{73}\right) = \left(\frac{3}{73}\right)^2 = +1.$$

Следовательно,

$$\left(\frac{438}{593}\right) = 1 \cdot (-1) \cdot 1 = -1.$$

Таким образом, сравнение $x^2 \equiv 438 \pmod{593}$ не имеет решений.

Можно было бы в этом примере поступить так: $438 \equiv -155 \pmod{593}$; $155 = 5 \cdot 31$, следовательно,

$$\left(\frac{438}{593}\right) = \left(\frac{-155}{593}\right) = \left(\frac{-1}{593}\right)\left(\frac{5}{593}\right)\left(\frac{31}{593}\right) = \left(\frac{5}{593}\right)\left(\frac{31}{593}\right), \text{ ибо } \left(\frac{-1}{593}\right) = +1.$$

Далее:

$$\left(\frac{5}{593}\right) = \left(\frac{593}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1;$$

$$\left(\frac{31}{593}\right) = \left(\frac{593}{31}\right) = \left(\frac{4}{31}\right) = \left(\frac{2}{31}\right)^2 = +1.$$

Следовательно,

$$\left(\frac{438}{593}\right) = -1.$$

Пример 2. Вычислить $\left(\frac{2023}{1231}\right)$. Сначала приведем числитель по модулю 1231:

$$\left(\frac{2023}{1231}\right) = \left(\frac{792}{1231}\right);$$

разложим 792 на простые множители: $792 = 2^3 \cdot 3^2 \cdot 11$;

$$\left(\frac{792}{1231}\right) = \left(\frac{2^3}{1231}\right)\left(\frac{3^2}{1231}\right)\left(\frac{11}{1231}\right) = \left(\frac{2}{1231}\right)\left(\frac{11}{1231}\right);$$

$\left(\frac{2}{1231}\right) = +1$, ибо 1231 вида $8k + 7$.

$$\left(\frac{11}{1231}\right) = -\left(\frac{1231}{11}\right),$$

ибо здесь оба числа 1231 и 11 вида $4k+3$; далее:

$$\left(\frac{1231}{11}\right)=\left(\frac{-1}{11}\right)=-1, \text{ ибо 11 вида } 4k+3 \text{ (см. § 48, IV).}$$

Следовательно,

$$\left(\frac{792}{1231}\right)=+1,$$

т. е. сравнение $x^2 \equiv 792 \pmod{1231}$ имеет решения.

§ 50. Символ Якоби. При вычислении символа Лежандра наибольшую трудность представляет разложение числителя на простые множители; в случае, если числитель весьма большое число, разложение может оказаться практически невыполнимым. Чтобы избежать этого разложения, Якоби обобщил символ Лежандра на случай, когда знаменатель — составное нечетное число; это обобщение и называется символом Якоби.

Пусть P — любое нечетное положительное число и a взаимно-простое с P; пусть $P=pp'p''\ldots$ разложение числа P на простые множители (p, p', p'', ... не обязательно все различны). В таком случае *определим*:

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p}\right)\left(\frac{a}{p'}\right)\left(\frac{a}{p''}\right)\ldots, \tag{114}$$

где $\left(\frac{a}{p}\right)$, $\left(\frac{a}{p'}\right)$, $\left(\frac{a}{p''}\right)$, ... обычные символы Лежандра (a, будучи взаимно-простым с P, взаимно-простое и с p, и с p', и с p'', ...); символ $\left(\frac{a}{P}\right)$ и есть символ Якоби.

Пусть $a=qq'q''\ldots$ разложение числа a на простые множители (q, q', q'', ... все отличны от p, p', p'', ... так как a и P взаимно-простые). Тогда (по I, § 48):

$$\left(\frac{a}{p}\right)=\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right)\left(\frac{q''}{p}\right)\ldots; \quad \left(\frac{a}{p'}\right)=\left(\frac{q}{p'}\right)\left(\frac{q'}{p'}\right)\left(\frac{q''}{p'}\right)\ldots; \text{ и т. д.}$$

Следовательно,

$$\left(\frac{a}{P}\right)=\prod_{p,\,q}\left(\frac{q}{p}\right). \tag{114a}$$

Произведение здесь берется по всем числам p, p', p'', ... и по всем числам q, q', q'', ... (так что каждое q комбинируется с каждым p). Соединяя в (114a) все множители с одним и тем же q, затем все множители с одним и тем же q' и т. д., получим (по определению символа Якоби):

$$\left(\frac{a}{P}\right)=\left(\frac{q}{P}\right)\left(\frac{q'}{P}\right)\left(\frac{q''}{P}\right)\ldots,$$

а это непосредственно приводит к свойству II, § 48:

$$\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right), \tag{115}$$

которое, таким образом (со всеми следствиями), доказано и для символов Якоби.

Из самого определения символа Якоби вытекает еще такое его свойство:

$$\left(\frac{a}{P_1 P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right), \tag{116}$$

если P_1 и P_2 взаимно-простые с a; это непосредственно обобщается и на несколько сомножителей в знаменателе.

Из определения (114) при $a = 1$ непосредственно вытекает:

$$\left(\frac{1}{P}\right) = +1. \tag{117}$$

Докажем теперь следующую лемму:

Лемма. Если P и P' нечетные числа, то:

1) $$\frac{PP' - 1}{2} \equiv \frac{P-1}{2} + \frac{P'-1}{2} \pmod 2; \tag{118}$$

2) $$\frac{(PP')^2 - 1}{8} \equiv \frac{P^2-1}{8} + \frac{P'^2-1}{8} \pmod 2. \tag{119}$$

Доказательство.

1) $(P-1)(P'-1)$ делится на 4; имеем:

$$(P-1)(P'-1) = PP' - P - P' + 1 =$$
$$= (PP'-1) - (P-1) - (P'-1) \equiv 0 \pmod 4;$$
$$PP' - 1 \equiv (P-1) + (P'-1) \pmod 4,$$

а отсюда, разделив обе части и модуль на 2, получим (118).

2) Имеем (по теореме 52, § 34): $P^2 - 1$ и $P'^2 - 1$ делятся на 8, следовательно, $(P^2-1)(P'^2-1)$ делится на 64. Таким образом:

$$(P^2-1)(P'^2-1) = P^2P'^2 - P^2 - P'^2 + 1 =$$
$$= [(PP')^2 - 1] - (P^2-1) - (P'^2-1) \equiv 0 \pmod{64}.$$

Деля обе части и модуль на 8, получим:

$$\frac{(PP')^2-1}{8} \equiv \frac{P^2-1}{8} + \frac{P'^2-1}{8} \pmod 8,$$

а значит это сравнение верно и для модуля 2, и мы получим (119).

Обе формулы (118) и (119) непосредственно обобщаются на случай нескольких нечетных чисел. Таким образом, если нечетное положительное число P разложено на простые множители $P = pp'p'' \ldots$, то:

$$\sum_p \frac{p-1}{2} \equiv \frac{P-1}{2} \pmod 2; \tag{118a}$$

$$\sum_p \frac{p^2-1}{8} \equiv \frac{P^2-1}{8} \pmod 2. \tag{119a}$$

При помощи этих формул легко доказать, что и свойства IV и V § 48 остаются верными для символов Якоби. Именно:

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p}\right)\left(\frac{-1}{p'}\right)\left(\frac{-1}{p''}\right)\ldots=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p'-1}{2}}\cdot(-1)^{\frac{p''-1}{2}}\ldots=$$

$$=(-1)^{\sum\frac{p-1}{2}}=(-1)^{\frac{P-1}{2}};$$

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p}\right)\left(\frac{2}{p'}\right)\left(\frac{2}{p''}\right)\ldots=(-1)^{\frac{p^2-1}{8}}\cdot(-1)^{\frac{p'^2-1}{8}}\cdot(-1)^{\frac{p''^2-1}{8}}\ldots=$$

$$=(-1)^{\sum\frac{p^2-1}{8}}=(-1)^{\frac{P^2-1}{8}}.$$

Легко доказать для символа Якоби и закон взаимности: пусть P и Q два положительных нечетных, взаимно-простых числа; $P=pp'p''\ldots$; $Q=qq'q''\ldots$ — их разложения на простые множители. Имеем по формуле (114a):

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=\prod_{p,\,q}\left(\frac{p}{q}\right)\cdot\prod_{p,\,q}\left(\frac{q}{p}\right)=\prod_{p,\,q}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\prod_{p,\,q}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}=$$

$$=(-1)^{\sum\limits_{p,q}\left(\frac{p-1}{2}\frac{q-1}{2}\right)}=(-1)^{\sum\limits_{p}\frac{p-1}{2}\cdot\sum\limits_{q}\frac{q-1}{2}}=(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

(по формуле (118a), примененной для P и для Q); это и есть закон взаимности.

Докажем и свойство I § 48 для символа Якоби. Если $P=pp'p''\ldots$, a — взаимно-простое с P и $a\equiv b\pmod P$, то, очевидно, и b взаимно-простое с P и верны такие сравнения: $a\equiv b\pmod p$, $a\equiv b\pmod{p'}$, $a\equiv b\pmod{p''}$ и т. д.; следовательно,

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right),\quad\left(\frac{a}{p'}\right)=\left(\frac{b}{p'}\right),\quad\left(\frac{a}{p''}\right)=\left(\frac{b}{p''}\right),\ \ldots$$

Перемножая эти равенства, найдем по (114):

$$\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right),$$

что и требуется доказать.

Итак:

Теорема 75. Для символов Якоби верны свойства I—V § 48 и закон взаимности.

Таким образом, символы Якоби вычисляются по тем самым правилам, что и символы Лежандра. Вообще, при вычислении нам не нужно отличать символы Якоби от символов Лежандра, являющихся просто частными случаями символов Якоби. Этим мы при вычислении символов Лежандра избавились от необходимости разложения числителей на простые множители; нужно только выделить множители $=2$.

Замечание. Теорема 75 доказывает, что для обобщения Якоби символа Лежандра выполнен так называемый «принцип

перманентности». Этот принцип требует, чтобы при обобщении данного понятия оставались верными основные свойства этого понятия. Можно было бы полагать, что более натуральным обобщением символа Лежандра для составного знаменателя являлось бы такое: считать $\left(\frac{a}{P}\right)=+1$, если сравнение $x^2 \equiv a \pmod P$ имеет решение; в противном случае считать $\left(\frac{a}{P}\right)=-1$. Но тогда не был бы выполнен принцип перманентности и такое обобщение не имело бы никакого практического значения. Заметим, что для символа Якоби условие $\left(\frac{a}{P}\right)=+1$ необходимо, но недостаточно для того, чтобы сравнение $x^2 \equiv a \pmod P$ имело решение (см. ниже, § 57, теорему 81).

Пример 1. Вычислить $\left(\frac{853}{1409}\right)$. Вычисляем, не заботясь о том, какие промежуточные символы мы получаем,— Лежандра или Якоби.

$$\left(\frac{853}{1409}\right)=\left(\frac{1409}{853}\right)=\left(\frac{556}{853}\right)=\left(\frac{2^2}{853}\right)\left(\frac{139}{853}\right)=\left(\frac{139}{853}\right)=\left(\frac{853}{139}\right)=\left(\frac{19}{139}\right)=$$
$$=-\left(\frac{139}{19}\right)=-\left(\frac{6}{19}\right)=-\left(\frac{2}{19}\right)\left(\frac{3}{19}\right)=\left(\frac{3}{19}\right)=-\left(\frac{19}{3}\right)=-\left(\frac{1}{3}\right)=-1.$$

Пример 2. Вычислить $\left(\frac{5381}{6277}\right)$. Имеем:

$$\left(\frac{5381}{6277}\right)=\left(\frac{-896}{6277}\right)=\left(\frac{-1}{6277}\right)\left(\frac{2^7}{6277}\right)\left(\frac{7}{6277}\right)=\left(\frac{2}{6277}\right)\left(\frac{7}{6277}\right)=-\left(\frac{6277}{7}\right)=$$
$$=-\left(\frac{5}{7}\right)=-\left(\frac{7}{5}\right)=-\left(\frac{2}{5}\right)=+1.$$

§ 51. Символы Лежандра и Якоби дают ответ на вопрос: возможно ли сравнение:

$$x^2 \equiv a \pmod p, \tag{104a}$$

где p — простое, a не делится на p. При данных числах a и p требуется только вычислить символ Лежандра $\left(\frac{a}{p}\right)$. Пусть теперь одно из чисел a, p неопределенное (переменное); в таком случае возникают такие две задачи:

1. Дано число p; найти все числа a, для которых $\left(\frac{a}{p}\right)=+1$, т. е. сравнение (104a) возможно; иными словами, найти все квадратичные вычеты числа p. Эта задача конечна, ибо a вообще может иметь только $p-1$ различных значений (по модулю p): $1, 2, 3, \ldots$ $\ldots\ p-1$. Каждое из этих значений a следует испытать, вычислив для него символ Лежандра $\left(\frac{a}{p}\right)$; половина этих значений a будут квадратичными вычетами числа p, половина — невычетами. Можно поступить и так: возвысить в квадрат каждое из чисел $1, 2, 3, \ldots p-1$ и взять наименьшие положительные вычеты этих квадратов по

модулю p. Эти вычеты и являются всеми квадратичными вычетами числа p; каждый из них встретится при этом два раза, ибо $\lambda^2 \equiv (p-\lambda)^2$; различных имеется как раз $\frac{p-1}{2}$. Можно даже взять не все числа 1, 2, ... $p-1$, а только первые $\frac{p-1}{2}$ чисел: 1, 2, 3, ... $\frac{p-1}{2}$; их квадраты и дадут все квадратичные вычеты числа p, и каждый по одному разу.

Примеры: 1) $p=3$; $p-1=2$; здесь имеется только один квадратичный вычет, а именно, 1 и один невычет $=2$.

2) $p=5$; для a имеется 4 значения: 1, 2, 3, 4; из них 1, 4 — вычеты, а 2, 3 — невычеты (заметим, что квадраты — всегда вычеты).

3) $p=7$; $a=1$, 2, 3, 4, 5, 6; беря квадраты чисел 1, 2, 3, найдем вычеты 1, 4, $9 \equiv 2$; невычеты: 3, 5, 6.

2. Гораздо труднее вторая задача: дано число a; найти все (нечетные простые) числа p, для которых a — квадратичный вычет, т. е. для которых сравнение (104а) возможно. Иными словами, найти все (простые нечетные) числа p, которые могут быть делителями формы x^2-a (при различных целых значениях x).

Вместо формы x^2-a возьмем однородную форму t^2-au^2, где t и u переменные (принимающие целые значения). Очевидно, что делители формы x^2-a являются также делителями однородной формы t^2-au^2; следует только взять $t=x$, $u=1$, чтобы свести эту последнюю форму к первой. Но если поставить условие $D(t, u)=1$, то можно сказать, что и обратно: при этом условии простые делители формы t^2-au^2 будут также делителями неоднородной формы x^2-a. Действительно, пусть при некоторых целых, взаимно-простых t и u форма t^2-au^2 делится на простое число p:

$$t^2-au^2 \equiv 0 \pmod{p}; \qquad (120)$$

число u не делится на p, так как иначе и t делилось бы на p, и u и t не были бы взаимно-простыми. Следовательно, можно найти v так (§ 39, теорема 60), чтобы было:

$$uv \equiv 1 \pmod{p}.$$

Умножим обе части (120) на v^2 и заменим u^2v^2 единицей; получим:

$$(tv)^2-a \equiv 0 \pmod{p};$$

следовательно, при $x=tv$ x^2-a делится на p.

Итак:

Теорема 76. Формы x^2-a и t^2-au^2 при $D(t, u)=1$ имеют одни и те же простые делители.

Таким образом, нашу задачу можно формулировать так: найти все простые делители формы t^2-au^2 (при $D(t, u)=1$). Множество этих делителей бесконечно, поэтому эта вторая задача сложнее, чем первая Ее можно решить, пользуясь символами Лежандра и Якоби, как мы покажем на примерах. Заметим, что при $a=-1$

и $a=2$ она уже решена: свойства IV и V (§ 48) символов Лежандра и Якоби дают ее решения для $a=-1$ и $a=2$. Простыми делителями формы t^2+u^2 при $D(t, u)=1$ являются все простые числа вида $4k+1$ (а также и число 2 — при $t=1$, $u=1$). Простыми делителями формы t^2-2u^2 при $D(t, u)=1$ являются все простые числа вида $8k+1$ и $8k+7$ (и число 2 — при $t=0$, $u=1$).

Пример 1. Найти все простые делители формы t^2-3u^2 (при $D(t, u)=1$). Здесь $a=3$; надо найти все простые числа p так, чтобы было: $\left(\frac{3}{p}\right)=+1$. Следует рассмотреть два случая:

1) p вида $4m+1$; тогда по закону взаимности

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right);$$

$\left(\frac{p}{3}\right)=+1$ только если $p\equiv 1 \pmod 3$ (см. выше, пример в этом параграфе). Следовательно, для p у нас такие условия:

$$p\equiv 1 \pmod 4,\quad p\equiv 1 \pmod 3.$$

Решим эту систему сравнений (§ 43); найдем общее решение:

$$p\equiv 1 \pmod{12},\ \text{т. е. } p=12k+1.$$

2) p вида $4m+3$; тогда по закону взаимности

$$\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right);$$

$\left(\frac{p}{3}\right)=-1$ при $p\equiv 2 \pmod 3$. Следовательно, имеем:

$$p\equiv 3 \pmod 4,\quad p\equiv 2 \pmod 3.$$

Общее решение:

$$p\equiv 11 \pmod{12},\ \text{т. е. } p=12k+11.$$

Кроме того, следует особо рассмотреть число 2 и простые делители числа a (в данном случае 3), ибо найденные нами числа p — нечетные и взаимно-простые с a. Но t^2-3u^2, очевидно, делится на 2 при $t=u=1$ и на 3 при $t=0$, $u=1$.

Таким образом, форма t^2-3u^2 имеет такие простые делители:

$$2,\ 3,\ 12k+1,\ 12k+11\ (\text{или } 12k-1).$$

Пример 2. Найти простые делители формы t^2+7u^2 (при $D(t, u)=1$). Здесь $a=-7$; следовательно, нужно исследовать символ $\left(\frac{-7}{p}\right)$.

Имеем (по свойству IV § 48 и по закону взаимности):

$$\left(\frac{-7}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{7}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}\cdot\frac{7-1}{2}}=(-1)^{\frac{p-1}{2}+3\frac{p-1}{2}}\cdot\left(\frac{p}{7}\right)=$$

$= \left(-1\right)^{2(p-1)} \left(\frac{p}{7}\right) = \left(\frac{p}{7}\right)$. Но, как мы видели в этом же параграфе, $\left(\frac{p}{7}\right) = +1$ при $p \equiv 1,\ 2,\ 4 \pmod 7$. Следовательно, p имеет одну из таких форм: $7k+1$, $7k+2$, $7k+4$; все простые числа этих форм являются делителями формы t^2+7u^2. Кроме того, делителями этой формы являются числа 2 (при $t=u=1$) и 7 (при $t=0,\ u=1$).

§ 52. Что касается фактического решения сравнений вида (104a), т. е. нахождения их корней, то до сих пор не существует практического способа этого решения без специальных таблиц. Конечно, можно всегда найти x хотя бы простыми пробами, ибо количество этих проб ограничено (надо испробовать только $p-1$ чисел $1, 2, \ldots p-1$ при данном модуле p); но при большом модуле этот способ оказывается совершенно непрактичным. Мы укажем два случая, когда самый критерий Эйлера дает общую формулу для нахождения решений сравнения (104a):

I. Пусть $p=4k+3$; когда $\frac{p-1}{2}=2k+1$, и по формуле (105) § 47 получим (предполагая, что наше сравнение имеет решения):

$$a^{2k+1} \equiv 1 \pmod p.$$

Умножая обе части на a, найдем:

$$a^{2k+2} \equiv a \pmod p$$

или:

$$(a^{k+1})^2 \equiv a \pmod p.$$

Следовательно, $x \equiv \pm a^{k+1}$ — искомое решение сравнения (104a).

II. Пусть $p=8k+5$; тогда $\frac{p-1}{2}=4k+2$. Формула (105) дает:

$$a^{4k+2} \equiv 1 \pmod p$$

или:

$$(a^{2k+1}-1)(a^{2k+1}+1) \equiv 0 \pmod p.$$

Если произведение делится на простое число p, то (по теореме 19, § 10) по крайней мере один из сомножителей должен делится на p; оба они вместе делиться на p не могут, так как их разность $=2$ — не делится на p. Следовательно, должен иметь место один из следующих двух случаев:

1) $a^{2k+1}-1 \equiv 0 \pmod p$, т. е. $a^{2k+1} \equiv 1 \pmod p$; но тогда $a^{2k+2} \equiv a \pmod p$ и $x \equiv \pm a^{k+1}$ — решение сравнения (104a).

2) $a^{2k+1}+1 \equiv 0 \pmod p$, т. е. $a^{2k+1} \equiv -1 \pmod p$; но тогда

$$a^{2k+2} \equiv -a \pmod p.$$

Возьмем какой-нибудь квадратичный невычет числа p; так как $p=8k+5$, то простейший такой невычет $=2$ (§ 48, V). Имеем по (105a):

$$2^{\frac{p-1}{2}} = 2^{4k+2} \equiv -1 \pmod p;$$

перемножив почленно два последних сравнения, найдем:

$$2^{4k+2}\cdot a^{2k+2}\equiv a\,(\mathrm{mod}\,p)$$

или

$$(2^{2k+1}\cdot a^{k+1})^2\equiv a\,(\mathrm{mod}\,p).$$

Следовательно, $x\equiv\pm 2^{2k+1}\cdot a^{k+1}$ — решение сравнения (104а).

Но надо заметить, что при большом p эти решения практически так же неудобны, как и применение критерия Эйлера.

§ 53. При $p=8k+1$ нет готовой формулы для решения сравнения (104а). В следующей главе мы увидим, что сравнения вида (104а) легко решить при помощи так называемых индексов, но для этого требуются специальные таблицы. Есть еще способ А. Н. Коркина решения двучленных сравнений вида

$$x^n\equiv a\,(\mathrm{mod}\,p),$$

но этот способ требует тоже наличия специальных таблиц. В общем виде он изложен в учебнике Д. А. Граве «Элементарный курс теории чисел» (Киев, 1913, гл. IV). Мы изложим частный случай способа Коркина — для квадратных сравнений вида (104а), где p вида $8k+1$.

Положим для общности

$$p=2^{\lambda}k+1,$$

где $\lambda\geqq 3$, k — нечетное.

Рассмотрим ряд сравнений:

$$\left.\begin{array}{l} z_1^2\equiv -1\,(\mathrm{mod}\,p);\; z_2^{2^2}\equiv -1\,(\mathrm{mod}\,p);\; z_3^{2^3}\equiv -1\,(\mathrm{mod}\,p);\ldots \\ \ldots\; z_{\lambda-1}^{2^{\lambda-1}}\equiv -1\,(\mathrm{mod}\,p). \end{array}\right\}\quad (121)$$

Пусть f — квадратичный невычет числа p; по (105а), § 47, имеем:

$$f^{\frac{p-1}{2}}=f^{2^{\lambda-1}k}\equiv -1\,(\mathrm{mod}\,p). \qquad (122)$$

Это можно написать так:

$$\left(f^{2^{\lambda-2}k}\right)^2\equiv -1\,(\mathrm{mod}\,p);$$

следовательно, $u_{11}\equiv f^{2^{\lambda-2}k}$ и $u_{12}\equiv -f^{2^{\lambda-2}k}$ являются решениями первого сравнения (121). Оба эти решения различны: если бы $f^{2^{\lambda-2}k}\equiv -f^{2^{\lambda-2}k}\,(\mathrm{mod}\,p)$, то $2f^{2^{\lambda-2}k}$ делилось бы на p тогда как ни 2, ни f на p не делится. Напишем теперь (122) в следующем виде:

$$\left(f^{2^{\lambda-3}k}\right)^{2^2}\equiv -1\,(\mathrm{mod}\,p).$$

Отсюда видно, что $u_{21}\equiv f^{2^{\lambda-3}k}$ и $u_{22}\equiv -u_{21}$ являются решениями второго сравнения (121); как и перед тем, докажем, что эти решения различны. Но и $u_{23}\equiv u_{11}u_{21}$, и $u_{24}\equiv -u_{11}u_{21}$ тоже решения второго сравнения (121), так как $u_{21}^{2^2}\equiv -1$, $u_{11}^{2^2}\equiv +1\,(\mathrm{mod}\,p)$.

Все найденные четыре решения различны: пусть $u_{21} \equiv \pm u_{23} \pmod p$ или $u_{21} \equiv \pm u_{11}u_{21} \pmod p$; сократим на u_{21} (ибо u_{21} не делится на p); получим: $u_{11} \equiv \pm 1 \pmod p$, что́ неверно, так как тогда было бы: $u_{11}^2 \equiv +1$, а на самом деле $u_{11}^2 \equiv -1$.

Написав теперь (122) в виде

$$\left(f^{2^{\lambda-4}k}\right)^{2^3} \equiv -1 \pmod p,$$

найдем решения третьего сравнения (121): $u_{31} \equiv f^{2^{\lambda-4}k}$, $u_{32} \equiv -u_{31}$. Остальные шесть решений третьего сравнения (121) найдутся умножением u_{31} на все решения предыдущих двух сравнений (121). Как и в предыдущем случае, можно доказать, что все найденные таким образом восемь решений 3-го сравнения (121) различны.

Вообще, чтобы найти все решения μ-го сравнения (121)

$$z_\mu^{2^\mu} \equiv -1 \pmod p, \tag{121a}$$

перепишем (122) таким образом:

$$\left(f^{2^{\lambda-\mu-1}k}\right)^{2^\mu} \equiv -1 \pmod p.$$

Отсюда видно, что $u_{\mu 1} \equiv f^{2^{\lambda-\mu-1}k}$, $u_{\mu 2} \equiv -u_{\mu 1}$ являются решениями сравнения (121a); остальные его решения найдутся умножением $u_{\mu 1}$ на каждое решение всех предыдущих сравнений. Всего получим, таким образом, $2 + 2^2 + 2^3 + \ldots + 2^{\mu-1} = 2^\mu - 2$ решения; вместе с двумя решениями $u_{\mu 1}$, $u_{\mu 2}$ это даст 2^μ решений. Все они различны по модулю p. Пусть именно:

$$u_{\mu 1}u_{\varkappa\lambda} \equiv u_{\mu 1}u_{\rho\sigma} \pmod p,$$

где $\varkappa < \mu$, $\rho < \mu$. Так как $u_{\mu 1}$ не делится на p, то полученное сравнение можно на $u_{\mu 1}$ сократить:

$$u_{\varkappa\lambda} \equiv u_{\rho\sigma} \pmod p;$$

но это сравнение невозможно: при $\varkappa = \rho$ и $\lambda \neq \sigma$ $u_{\varkappa\lambda}$ и $u_{\varkappa\sigma}$ различные по модулю p решения $\varkappa$-го сравнения (121), а при $\varkappa \neq \rho$, например, при $\varkappa < \rho$ $u_{\varkappa\lambda}$ и $u_{\rho\sigma}$ не сравнимы по модулю p, потому что $u_{\rho\sigma}^{2^\rho} \equiv -1$, тогда как $u_{\varkappa\lambda}^{2^\rho} \equiv +1 \pmod p$.

Абсолютно-наименьшие вычеты решений всех сравнений (121) Коркин назвал *квадратичными характеристиками* числа p. Он составил их таблицы для простых чисел $p < 5000$, К. А. Поссе продолжил их для $p < 10000$. Мы будем обозначать эти абсолютно-наименьшие вычеты буквою u с двумя значками, из которых первый есть номер сравнения (121). Возьмем все μ-е квадратичные характеристики:

$$u_{\mu 1},\ u_{\mu 2},\ \ldots\ u_{\mu 2^\mu}; \tag{123}$$

очевидно, что их квадраты удовлетворяют сравнению

$$z_{\mu-1}^{2^{\mu-1}} \equiv -1 \pmod p,$$

т. е. сравнимы с $(\mu-1)$-ми квадратичными характеристиками:

$$u_{\mu-1,1},\ u_{\mu-1,2},\ \ldots\ u_{\mu-1,2^{\mu-1}}. \qquad (123a)$$

Посмотрим, в каком случае $u_{\mu x}^2 \equiv u_{\mu\lambda}^2 \pmod p$. Для этого должно быть:

$$(u_{\mu x} - u_{\mu\lambda})(u_{\mu x} + u_{\mu\lambda}) \equiv 0 \pmod p,$$

т. е. или $u_{\mu x} \equiv u_{\mu\lambda}$ (это одна и та же характеристика), или $u_{\mu x} \equiv -u_{\mu\lambda} \pmod p$. С другой стороны, $-u_{\mu\lambda}$ ведь тоже решение сравнения (121а), отличное от $u_{\mu\lambda}$, т. е. сравнимое с некоторой характеристикой (123). Следовательно, квадраты всех характеристик (123) являются всеми $2^{\mu-1}$ решениями $(\mu-1)$-го сравнения (121).

Отсюда следует: всякая $(\mu-1)$-я квадратичная характеристика (123а) непременно сравнима с квадратом некоторой μ-ой характеристики (123) (даже не одной, а двух).

Обратимся теперь к нашему сравнению:

$$x^2 \equiv a \pmod p,$$

где $p = 2^\lambda k + 1$; k — нечетное. Пусть $\left(\frac{a}{p}\right) = +1$, т. е. по критерию Эйлера $a^{\frac{p-1}{2}} = a^{2^{\lambda-1}k} \equiv 1 \pmod p$.

Докажем, что или $a^k \equiv 1 \pmod p$, или в ряде

$$a^{2^{\lambda-2}k},\quad a^{2^{\lambda-3}k},\ \ldots\ a^{2k},\ a^k$$

непременно найдется число, сравнимое с -1 по модулю p.

Именно из критерия Эйлера следует:

$$a^{2^{\lambda-1}k} - 1 = \left(a^{2^{\lambda-2}k} - 1\right)\left(a^{2^{\lambda-2}k} + 1\right) \equiv 0 \pmod p;$$

один из сомножителей левой части должен делиться на p (оба они одновременно не могут делиться на p, так как их разность $= 2$). Если $a^{2^{\lambda-2}k} + 1$ делится на p, то наше утверждение доказано. Если же $a^{2^{\lambda-2}k} - 1 = \left(a^{2^{\lambda-3}k} - 1\right)\left(a^{2^{\lambda-3}k} + 1\right)$ делится на p, то или $a^{2^{\lambda-3}k} + 1$ делится на p и наше утверждение доказано, или $a^{2^{\lambda-3}k} - 1 = \left(a^{2^{\lambda-4}k} - 1\right)\left(a^{2^{\lambda-4}k} + 1\right)$ делится на p, и мы далее рассуждаем подобно же. Т. е., в конце концов, мы найдем, что или $a^{2^{\lambda-s}k} + 1$ делится на p (где s — одно из чисел $2, 3, \ldots \lambda$), или $a^k - 1$ делится на p.

Разберем такие случаи:

1) $a^k \equiv 1 \pmod p$, тогда: $a^{k+1} = \left(a^{\frac{k+1}{2}}\right)^2 \equiv a \pmod p$ (k — нечетное), т. е. $\pm a^{\frac{k+1}{2}}$ — решения нашего сравнения.

2) $a^k \equiv -1 \pmod p$; $\left(a^{\frac{k+1}{2}}\right)^2 \equiv -a \pmod p$. Пусть f — любой квадратичный невычет числа p; тогда $f^{\frac{p-1}{2}} = f^{2^{\lambda-1}k} \equiv -1 \pmod p$;

$\left(f^{2^{\lambda-2}k}a^{\frac{k+1}{2}}\right)^2 \equiv a \pmod{p}$, т. е. $\pm f^{2^{\lambda-2}k}a^{\frac{k+1}{2}}$ — решения нашего сравнения.

3) $a^{2^{\lambda-s}k} \equiv -1 \pmod{p}$, где $2 \leq s < \lambda$, или иначе:

$$(a^k)^{2^{\lambda-s}} \equiv -1 \pmod{p}.$$

Следовательно, a^k — одно из решений $(\lambda - s)$-го сравнения (121) и по доказанному выше

$$a^k \equiv b^2 \pmod{p}, \tag{124}$$

где b — решение $(\lambda - s + 1)$-го сравнения (121). Умножая (124) на a, найдем:

$$\left(a^{\frac{k+1}{2}}\right)^2 \equiv ab^2 \pmod{p}.$$

Найдем t из сравнения $bt \equiv 1 \pmod{p}$ (t существует, так как b не делится на p) и получим:

$$\left(a^{\frac{k+1}{2}} \cdot t\right)^2 \equiv a \pmod{p},$$

т. е. $\pm a^{\frac{k+1}{2}} \cdot t$ и являются решениями данного сравнения.

Пример 1. Решить сравнение $x^2 \equiv 11 \pmod{43}$.

Вычисляем: $\left(\frac{11}{43}\right) = -\left(\frac{43}{11}\right) = -\left(\frac{-1}{11}\right) = +1$, следовательно, сравнение имеет решение.

Здесь $43 = 4 \cdot 10 + 3$; мы имеем случай 1; $k = 10$, $k + 1 = 11$, следовательно, $x \equiv \pm 11^{11} \pmod{43}$.

Вычисляем: $11^2 = 121 \equiv -8 \pmod{43}$;
$11^4 \equiv 64 \equiv 21$;
$11^8 \equiv 441 \equiv 11$;
$11^{10} \equiv -8 \cdot 11 \equiv -88 \equiv -2$;
$11^{11} \equiv -22 \equiv 21$;

следовательно, $x \equiv \pm 21 \pmod{43}$.

Пример 2. Решить сравнение $x^2 \equiv 7 \pmod{29}$.

Здесь: $29 = 8 \cdot 3 + 5$; мы имеем случай II; $k = 3$. Вычисляем:

$$\left(\frac{7}{29}\right) = \left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = +1; \quad 2k + 1 = 7; \quad k + 1 = 4;$$

$7^2 = 49 \equiv -9 \pmod{29}$;
$7^4 \equiv 81 \equiv -6$;
$7^6 \equiv (-9)(-6) = 54 \equiv -4$;
$7^7 \equiv -28 \equiv +1$;

следовательно, $x \equiv \pm 7^{k+1} = \pm 7^4$, или $x \equiv \pm 6 \pmod{29}$.

Пример 3. Решить сравнение $x^2 \equiv 23 \pmod{101}$.

Здесь: $\left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = +1$. Далее: $101 = 8 \cdot 12 + 5$ (случай II);

$k = 12,\quad 2k + 1 = 25,\quad k + 1 = 13$. Имеем:

$$\begin{aligned} 23^2 &= 529 \equiv 24 \pmod{101};\\ 23^4 &\equiv 576 \equiv -30;\\ 23^{12} &\equiv -27000 \equiv -33;\\ 23^{13} &\equiv -33 \cdot 23 = -759 \equiv 49;\\ 23^{25} &\equiv -33 \cdot 49 = -1617 \equiv -1; \end{aligned}$$

следовательно, $x \equiv \pm 2^{2k+1} \cdot 23^{k+1} = \pm 2^{25} \cdot 23^{13}$;

$$2^5 = 32;\ 2^{10} = 1024 \equiv 14 \pmod{101};\ 2^{20} \equiv 196 \equiv -6;$$
$$2^{25} \equiv -6 \cdot 32 = -192 \equiv 10;$$

таким образом, $x \equiv \pm 10 \cdot 49 = \pm 490 \equiv \pm 15 \pmod{101}$.

Пример 4. Решить сравнение $x^2 \equiv 2 \pmod{17}$.

Здесь: $\left(\frac{2}{17}\right) = +1$; $17 = 2^4 \cdot 1 + 1$. Имеем сравнения (121)

$$z_1^2 \equiv -1 \pmod{17},\ z_2^{2^2} \equiv -1 \pmod{17},\quad z_3^{2^3} \equiv -1 \pmod{17}.$$

Здесь $f = -3$ квадратичный невычет по модулю 17. По критерию Эйлера $(-3)^8 = (-3)^{2^3} \equiv -1 \pmod{17}$; $(-3)^4 \equiv -4$; следовательно, $u_{11} \equiv 4$, $u_{12} \equiv -4$; $(-3)^2 \equiv 9 \equiv -8$; следовательно, $u_{21} \equiv 8$, $u_{22} \equiv -8$, $u_{23} \equiv 32 \equiv -2$, $u_{24} \equiv 2$. Наконец: $u_{31} \equiv 3$, $u_{32} \equiv -3$, $u_{33} \equiv 7$, $u_{34} \equiv -7$, $u_{35} \equiv 6$, $u_{36} \equiv -6$, $u_{37} \equiv 5$, $u_{38} \equiv -5$. У нас $a = 2$; находим: $2^{2^2} \equiv -1 \pmod{17}$; следовательно, 2 сравнимо с квадратом одного из решений сравнения $z_3^{2^3} \equiv -1 \pmod{17}$. Найдем: $2 \equiv 6^2 \pmod{17}$; так как здесь $k = 1$, то сразу получаем решение:

$$x \equiv \pm 6 \pmod{17}.$$

Пример 5. Решить сравнение $x^2 \equiv 5 \pmod{41}$.

Здесь: $\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = +1$; $41 = 2^3 \cdot 5 + 1$; $k = 5$.

Легко убедиться, что $f = 3$ — квадратичный невычет по модулю 41. Имеем сравнения (121):

$$z_1^2 \equiv -1 \pmod{41},\quad z_2^{2^2} \equiv -1 \pmod{41};$$

решения их: $z_1 \equiv \pm 9$; $z_2 \equiv \pm 3,\ \pm 14$.

Далее:

$a^k = 5^5 = 3125 \equiv 9 \pmod{41}$; $a^{2k} = 5^{10} \equiv -1$, т. е. $9^2 \equiv -1$, $b = 3$.

Теперь решаем сравнение: $3t \equiv 1 \pmod{41}$; находим: $t \equiv 14$; $a^{\frac{k+1}{2}} \equiv 5^3 = 125 \equiv 2$; $x \equiv 2 \cdot 14 = 28 \equiv -13$; следовательно,

$$x \equiv \pm 13 \pmod{41}.$$

§ 54. Рассмотрим теперь сравнение вида

$$x^2 \equiv a \pmod{p^\alpha}, \qquad (104)$$

где $\alpha > 1$ — целое число, а p — простое нечетное число. Рассмотрим случай, когда a не делится на p, т. е. когда $D(a, p^{\alpha}) = 1$. Если сравнение (104) имеет решения, то эти решения удовлетворяют и сравнению

$$x^2 \equiv a \pmod{p}, \tag{104a}$$

так как $x^2 - a$, делясь на p^{α}, делится и на p. А сравнение (104a) имеет решения тогда и только тогда, когда

$$\left(\frac{a}{p}\right) = +1;$$

следовательно, это условие необходимо для разрешимости сравнения (104). Мы докажем, что оно и достаточно. Пусть оно выполнено; тогда сравнение (104a) имеет решение, следовательно,

$$b^2 \equiv a \pmod{p},$$

или:

$$b^2 - a = kp,$$

где k — целое число. Возвышая обе части последнего равенства в α-ю степень, найдем:

$$(b^2 - a)^{\alpha} = k^{\alpha} p^{\alpha} \equiv 0 \pmod{p^{\alpha}}. \tag{125}$$

Имеем (по формуле бинома Ньютона):

$$\left(b + \sqrt{a}\right)^{\alpha} = b^{\alpha} + \alpha b^{\alpha-1}\sqrt{a} + \binom{\alpha}{2} b^{\alpha-2}a + \binom{\alpha}{3} b^{\alpha-3}a\sqrt{a} + \binom{\alpha}{4} b^{\alpha-4}a^2 + \ldots$$

Можно соединить отдельно все члены, не имеющие корня, и отдельно все члены, имеющие множитель $\sqrt{a}$; получим такое выражение:

$$\left(b + \sqrt{a}\right)^{\alpha} = t + v\sqrt{a}, \tag{126}$$

где t и v — целые числа. Взяв $b - \sqrt{a}$ вместо $b + \sqrt{a}$, мы только изменим знаки у всех членов, которые имеют множитель $\sqrt{a}$, следовательно,

$$\left(b - \sqrt{a}\right)^{\alpha} = t - v\sqrt{a}, \tag{126a}$$

а отсюда, перемножив (126) и (126a), получим:

$$(b^2 - a)^{\alpha} = t^2 - av^2.$$

Подставляя это в (125), получим:

$$t^2 - av^2 \equiv 0 \pmod{p^{\alpha}},$$

или:

$$t^2 \equiv av^2 \pmod{p^{\alpha}}. \tag{127}$$

Докажем, что t, а значит и v, не делятся на p. Для этого сложим почленно (126) и (126а):

$$t = \frac{1}{2}\left[(b + \sqrt{a})^\alpha + (b - \sqrt{a})^\alpha\right] = f(a, b).$$

Мы обозначили правую часть через $f(a, b)$; это — некоторая целая рациональная функция от a и b с целыми коэффициентами, ибо, как легко видеть, члены, имеющие множитель $\sqrt{a}$, сокращаются, а члены без множителя $\sqrt{a}$ удваиваются. Но b — корень сравнения (104а), т. е. $b^2 \equiv a \pmod{p}$, а потому:

$$t = f(a, b) \equiv f(b^2, b) \pmod{p}$$

(§ 33, теорема 51). Но при $a = b^2$ получаем:

$$f(b^2, b) = \frac{1}{2}\left[(b + b)^\alpha + (b - b)^\alpha\right] = \frac{1}{2}(2b)^\alpha = 2^{\alpha-1}b^\alpha;$$

таким образом,

$$t \equiv 2^{\alpha-1}b^\alpha \pmod{p}.$$

Правая часть этого сравнения $2^{\alpha-1}b^\alpha$ взаимно-простая с p, ибо p нечетное, а b, как корень сравнения (104а), где a не делится на p, — тоже взаимно-простое с p. Следовательно, и t и v взаимно-простые с p, а значит, и с p^α. Таким образом, сравнение

$$tu \equiv a \pmod{p^\alpha}$$

имеет решение u (§ 39, теорема 60); отсюда:

$$t^2u^2 \equiv a^2 \pmod{p^\alpha}.$$

Умножив на u^2 сравнение (127), получим, заменив t^2u^2 через a^2,

$$a^2 \equiv av^2u^2 \pmod{p^\alpha},$$

или, сократив на a, взаимно-простое с p^α:

$$v^2u^2 \equiv a \pmod{p^\alpha}.$$

Следовательно,

$$x \equiv uv \pmod{p^\alpha} \tag{127a}$$

и есть решение сравнения (104), которое, таким образом, имеет решение.

Найдем число различных решений сравнения (104). Пусть c — одно из решений; очевидно, что $-c$ — тоже решение, отличное от c; ибо, если бы было $c \equiv -c \pmod{p^\alpha}$, то оказалось бы $2c \equiv 0 \pmod{p^\alpha}$, а это неверно, так как ни 2, ни c не делятся на p, т. е. взаимно-простые с p^α. Пусть теперь x — какое-нибудь решение сравнения (104); в таком случае

$$x^2 \equiv a \pmod{p^\alpha}, \text{ но в то же время и } c^2 \equiv a \pmod{p^\alpha}.$$

Отсюда:

$$x^2 - c^2 \equiv 0 \pmod{p^\alpha},$$

или:

$$(x - c)(x + c) \equiv 0 \pmod{p^\alpha}.$$

Пусть и $x - c$ и $x + c$ делятся на p; в таком случае и их разность $\pm 2c$ должна делиться на p, а это, как мы уже видели, наверно. Следовательно, из этих двух двучленов один делится на p^α, а другой взаимно-простой с p^α, т. е. или

$$x - c \equiv 0, \quad x \equiv c \pmod{p^\alpha},$$

или:

$$x + c \equiv 0, \quad x \equiv -c \pmod{p^\alpha}.$$

Кроме этих двух решений, иных нет. Таким образом:

Теорема 77. Сравнение (104) при a взаимно-простом с p^α имеет решения тогда и только тогда, когда сравнение (104а) имеет решения, т. е. когда $\left(\frac{a}{p}\right) = +1$, и при этом всегда два решения: $\pm x$, где x находится по формуле (127а).

Мы получили одновременно и способ нахождения решений сравнения (104), если известно решение b сравнения (104а).

Пример 1. Решить сравнение $x^2 \equiv 7 \pmod{27}$.

Сначала возьмем сравнение $x^2 \equiv 7 \pmod 3$, или (сводя 7 по модулю 3) $x^2 \equiv 1 \pmod 3$. Это сравнение разрешимо; одно из его решений: $b = 1$. Теперь находим по формуле бинома Ньютона:

$$(1 + \sqrt{7})^3 = 1 + 3\sqrt{7} + 21 + 7\sqrt{7} = 22 + 10\sqrt{7};$$

следовательно, $t = 22$, $v = 10$.

Далее решим сравнение

$$22u \equiv 7 \pmod{27} \text{ или } -5u \equiv -20 \pmod{27}.$$

Сократив на -5, получим:

$$u \equiv 4 \pmod{27}; \quad uv \equiv 40 \equiv 13;$$

следовательно,

$$x \equiv \pm 13 \pmod{27}.$$

Пример 2. Решить сравнение $x^2 \equiv 39 \pmod{625}$. Здесь: $625 = 5^4$. Возьмем сравнение $x^2 \equiv 39 \pmod 5$ или $x^2 \equiv 4 \pmod 5$; одно из его решений: $b = 2$. Далее находим:

$$(2 + \sqrt{39})^4 = 16 + 32\sqrt{39} + 24 \cdot 39 + 8 \cdot 39\sqrt{39} + 39^2 =$$
$$= 16 + 32\sqrt{39} + 936 + 312\sqrt{39} + 1521 = 2473 + 344\sqrt{39};$$

следовательно, $t = 2473$, $v = 344$. Затем решаем сравнение

$$2473u \equiv 39 \pmod{625},$$

или:

$$-27u \equiv 39 \pmod{625}.$$

Сокращаем на 3: $9u \equiv -13 \pmod{625}$, прибавляем к правой части 625:

$$9u \equiv 612 \pmod{625}.$$

Сокращая на 9, найдем: $u \equiv 68 \pmod{625}$;

$$uv \equiv 68 \cdot 344 = 23392 \equiv 267.$$

Следовательно,

$$x \equiv \pm 267 \pmod{625}.$$

§ 55. Теперь рассмотрим сравнение, у которого модуль — степень двух, вида

$$x^2 \equiv a \pmod{2^\alpha}; \qquad (128)$$

a — нечетное число, т. е. взаимно-простое с модулем.

Рассмотрим отдельно следующие случаи:

1) $\alpha = 1$, т. е. $x^2 \equiv a \pmod 2$.

Здесь только и может быть $a \equiv 1 \pmod 2$ (это и показывает, что a — любое нечетное число). Но тогда и x должен быть нечетным, ибо $x^2 - a$ — четное, т. е. $x \equiv 1 \pmod 2$. Но все нечетные числа образуют только один класс по модулю 2; следовательно, решение $x \equiv 1 \pmod 2$ — единственное.

2) $\alpha = 2$, т. е. $x^2 \equiv a \pmod 4$.

Здесь возможны два случая: $a \equiv 1$ или $a \equiv 3 \pmod 4$.

Очевидно, что x должно быть нечетным; но по теореме 52 (в § 34) квадрат всякого нечетного числа сравним с единицей по модулю 8, а следовательно, и по модулю 4. Отсюда следует, что при $a \equiv 3 \pmod 4$ наше сравнение не имеет решений, а при $a \equiv 1 \pmod 4$ ему удовлетворяют все нечетные числа x. Но по модулю 4 все нечетные числа образуют два класса, представителями которых служат числа 1 и 3; следовательно, в этом случае мы имеем два решения: $x \equiv 1$ и $x \equiv 3 \pmod 4$.

3) $\alpha = 3$, т. е. $x^2 \equiv a \pmod 8$.

Для a возможны значения: $a \equiv 1, 3, 5, 7 \pmod 8$; x — нечетное; т. е. по той же теореме 52 (§ 34) $x^2 \equiv 1 \pmod 8$. Следовательно, при $a \equiv 1 \pmod 8$ сравнение имеет четыре решения: $x \equiv 1, 3, 5, 7 \pmod 8$; в остальных же случаях, т. е. при $a \equiv 3, 5, 7$ решений нет.

4) $\alpha > 3$. Если сравнение (128) при $\alpha > 3$ имеет решения, то эти решения удовлетворяют тому же сравнению по модулю 8 (ибо $x^2 - a$, делясь на 2^α при $\alpha > 3$, делится и на 2^3). Но для этого должно быть, как мы видели в случае 3,

$$a \equiv 1 \pmod 8. \qquad (129)$$

Таким образом, это условие необходимо и при $\alpha > 3$. Мы докажем, что оно и достаточно. Но сначала выясним, сколько всего решений имеет сравнение (128), если оно вообще имеет решения. Пусть b — некоторое определенное его решение, а x — какое-нибудь его решение. Имеем:

$$b^2 \equiv a \pmod{2^\alpha}, \quad x^2 \equiv a \pmod{2^\alpha};$$

следовательно,

$$x^2 - b^2 \equiv 0 \pmod{2^\alpha}$$

или:

$$(x - b)(x + b) \equiv 0 \pmod{2^\alpha}.$$

Пусть:

$$x - b = 2^\varkappa k, \quad x + b = 2^\lambda l,$$

где k и l нечетные; тогда, складывая и деля на 2, получим:

$$x = 2^{\varkappa-1}k + 2^{\lambda-1}l.$$

Но x, как решение сравнения (128), должно быть нечетным; следовательно, или $\varkappa - 1$ или $\lambda - 1$ равно нулю, т. е. одно из чисел $\varkappa$, λ равно единице, а другое $\geqq \alpha - 1$ (ибо произведение $(x - b)(x + b)$ делится на 2^α).

Пусть $\lambda = 1$, тогда $\varkappa \geqq \alpha - 1$, и мы имеем:

$$x - b = 2^{\alpha-1}s,$$

где s — какое-нибудь (не обязательно нечетное) число, или

$$x = b + 2^{\alpha-1}s,$$

или, наконец,

$$x \equiv b + 2^{\alpha-1}s \pmod{2^\alpha}$$

(ибо решения сравнения (128) определяются по модулю 2^α). При четном s $x \equiv b \pmod{2^\alpha}$, при нечетном s $x \equiv b + 2^{\alpha-1} \pmod{2^\alpha}$; эти два решения различны по модулю 2^α.

Пусть теперь $\varkappa = 1$, а следовательно, $\lambda \geqq \alpha - 1$, и мы имеем:

$$x + b = 2^{\alpha-1}s,$$

где s — целое (не непременно нечетное) число. В этом случае, как и в предыдущем, мы найдем еще следующие два решения: $x \equiv -b \pmod{2^\alpha}$, $x \equiv -b + 2^{\alpha-1} \pmod{2^\alpha}$. Таким образом, сравнение (128) имеет всего четыре решения:

$$b, \ b + 2^{\alpha-1}, \ -b, \ -b + 2^{\alpha-1} \text{ (или } -b - 2^{\alpha-1});$$

эти все решения различны по модулю 2^α, в чем легко убедиться.

Докажем теперь, что условие (129) и достаточно для существования решений сравнения (128) при $\alpha > 3$. Мы видели, что это условие достаточно при $\alpha = 3$; следовательно, можно применить метод полной индукции. Пусть достаточность условия (129) доказана для сравнения

$$x^2 \equiv a \pmod{2^{\alpha-1}}, \qquad (128a)$$

т. е. при $a \equiv 1 \pmod 8$ это сравнение имеет решения. Если c — одно из его решений, то, как мы видели, остальные будут:

$$c + 2^{\alpha-2}, \ -c, \ -c + 2^{\alpha-2}.$$

Итак, $c^2 \equiv a \pmod{2^{\alpha-1}}$, т. е. $c^2 - a$ делится на $2^{\alpha-1}$ или $c^2 - a = 2^{\alpha-1}k$. Если k четное, то $c^2 - a$ делится и на 2^α, т. е. c — решение и сравнения (128), и наше утверждение доказано. Если же k — нечетное, то возьмем $(c + 2^{\alpha-2})^2 - a$; эта разность тоже де-

лится на $2^{\alpha-1}$, ибо $c+2^{\alpha-2}$ тоже решение сравнения (128a). Но мы имеем:

$$(c+2^{\alpha-2})^2-a=(c^2-a)+2^{\alpha-1}c+2^{2\alpha-4}=2^{\alpha-1}k+2^{\alpha-1}c+2^{2\alpha-4};$$

при $\alpha>3$ $2\alpha-4\geqq\alpha$; следовательно,

$$(c+2^{\alpha-2})^2-a\equiv 2^{\alpha-1}(k+c)\,(\mathrm{mod}\,2^{\alpha}).$$

Но k и c нечетные (k — по условию, c — как решение сравнения (128a) при нечетном a), следовательно, их сумма четная, а значит

$$(c+2^{\alpha-2})^2-a\equiv 0\,(\mathrm{mod}\,2^{\alpha}),$$

т. е. $c+2^{\alpha-2}$ — решение сравнения (128); наше утверждение доказано и в этом случае.

Таким образом, одно из решений сравнения (128a) является непременно и решением сравнения (128). Обозначим это решение через b; остальные решения сравнения (128), как мы видели: $-b$, $b+2^{\alpha-1}$, $-b+2^{\alpha-1}$. Все эти решения удовлетворяют и сравнению (128a), только для (128a) b и $b+2^{\alpha-1}$ (а также $-b$ и $-b+2^{\alpha-1}$) не различны, тогда как для сравнения (128) они различны; но решения b и $-b$ различны и для (128a).

Итак:

Теорема 78. Сравнение (128) при нечетном a имеет: 1) всегда одно решение при $\alpha=1$; 2) два решения при $\alpha=2$ и $a\equiv 1\pmod 4$ и ни одного при $\alpha=2$ и $a\equiv 3\pmod 4$; 3) при $\alpha\geqq 3$ (и нечетном a) сравнение (128) имеет решения только при $a\equiv 1\pmod 8$, и в этом случае четыре различных решения; два из них непременно удовлетворяют и сравнению $x^2\equiv a\,(\mathrm{mod}\,2^{\alpha+1})$.

Предыдущие рассуждения дают и метод решения сравнений (128) при $\alpha>3$.

Пример 1. $x^2\equiv 33\pmod{64}$. Здесь $a=33\equiv 1\pmod 8$, следовательно, решения имеются. Для нахождения их рассмотрим сравнения:

$$x^2\equiv 33\equiv 1\pmod 8;$$
$$x^2\equiv 33\equiv 1\pmod{16};$$
$$x^2\equiv 33\equiv 1\pmod{32};$$
$$x^2\equiv 33\pmod{64}.$$

Решения первого: 1, 3, 5, 7; из них 1 и 7 удовлетворяют и второму; остальные решения второго: $1+2^3$, $7+2^3$, т. е. все решения второго: 1, 7, 9, 15; из них 1 и 15 удовлетворяют третьему; остальные решения третьего: $1+2^4$, $15+2^4$, т. е. все решения третьего: 1, 15, 17, 31; из них 15 и 17 удовлетворяют и четвертому; остальные решения четвертого: $15+2^5$, $17+2^5$.

Таким образом, все решения данного сравнения:

15, 17, 47, 49.

Конечно, не нужно обязательно начинать со сравнения с модулем 8; следует начинать со сравнения с модулем 2^{α}, для которого нам известно хоть одно решение (остальные три решения легко найти). В данном примере это — третье сравнение, имеющее, очевидно, корень $= 1$.

Пример 2. $x^2 \equiv 89 \pmod{256}$. Здесь $a = 89 \equiv 1 \pmod 8$, т. е. решения имеются. Имеем: $89 \equiv 9 \pmod{16}$, $89 \equiv -7 \pmod{32}$, $89 \equiv 25 \pmod{64}$; 25 — точный квадрат. Заметим, что если в сравнении $x^2 \equiv a \pmod m$ с любым модулем a — точный квадрат, то такое сравнение всегда имеет решение: $x \equiv \sqrt{a}$. Значит, и у нас сравнение:

$$x^2 \equiv 25 \pmod{64}$$

имеет решение 5, и можно начать именно с этого сравнения.

Все его решения:

$$5,\ -5,\ 5 + 32 = 37,\ -5 + 32 = 27.$$

Легко проверить, что из этих решений 37 и 27 удовлетворяют и сравнению

$$x^2 \equiv 89 \pmod{128};$$

в частности, 37 удовлетворяет и сравнению

$$x^2 \equiv 89 \pmod{256}.$$

Таким образом, все корни этого последнего сравнения:

$$37,\ -37,\ 37 + 128 = 165,\ -37 + 128 = 91.$$

§ 56. Рассмотрим теперь случай, когда правая часть a нашего сравнения не взаимно-проста с модулем. Мы будем рассматривать вместе сравнения (104) и (128), т. е. будем считать p *каким-нибудь* простым числом,— нечетным или равным двум.

Пусть в сравнении (104) имеем: $a = p^{\lambda} a_1$, где a_1 не делится на p. Рассмотрим два случая:

I. $\lambda \geq \alpha$, следовательно, $a \equiv 0 \pmod p$ и наше сравнение имеет вид:

$$x^2 \equiv 0 \pmod{p^{\alpha}}. \qquad (130)$$

Здесь мы тоже различим два случая:

1) $\alpha = 2\beta$ — четное; чтобы x^2 делилось на p^{α}, нужно чтобы x делилось на p^{β}, т. е. $x \equiv k \cdot p^{\beta} \pmod{p^{\alpha}}$. При $k = 0, 1, 2, \ldots p^{\beta} - 1$ мы получаем различные (по модулю p^{α}) решения:

$$0,\ p^{\beta},\ 2p^{\beta},\ \ldots (p^{\beta} - 1)\, p^{\beta} = p^{\alpha} - p^{\beta};$$

число их есть p^{β}. При других целых значениях k мы получим решения, сравнимые с уже найденными. Таким образом, в этом случае сравнение (130) имеет $p^{\frac{\alpha}{2}}$ различных решений.

2) $\alpha = 2\beta + 1$ — нечетное; чтобы x^2 делилось на p^{α}, x должно

делиться на $p^{\beta+1}$; $x \equiv kp^{\beta+1} \pmod{p^\alpha}$. При $k = 0, 1, 2, \ldots p^\beta - 1$ мы получим различные решения (по модулю p^α):

$$0,\ p^{\beta+1},\ 2p^{\beta+1},\ \ldots (p^\beta - 1)\,p^{\beta+1} = p^\alpha - p^{\beta+1};$$

их число: $p^\beta = p^{\frac{\alpha-1}{2}}$. При других целых значениях k получим решения, сравнимые с уже найденными. Всего в этом случае сравнение (130) имеет $p^{\frac{\alpha-1}{2}}$ различных решений.

Итак:

Теорема 79. Сравнение (130) при любом простом p (включая и $p = 2$) имеет $p^{\left[\frac{\alpha}{2}\right]}$ различных по модулю p^α решений (ибо $\left[\frac{\alpha}{2}\right]$ равно $\frac{\alpha}{2}$ при четном α и $\frac{\alpha-1}{2}$ при нечетном α).

II. Пусть теперь $\lambda < \alpha$; наше сравнение имеет вид:

$$x^2 \equiv p^\lambda \cdot a_1 \pmod{p^\alpha}, \tag{131}$$

где a_1 не делится на p. Здесь мы тоже различим два случая:

1) $\lambda = 2\mu$ — четное; из (131) видно, что x^2 делится на p^λ, следовательно, x должно делиться на p^μ. Пусть $x = p^\mu z$; в таком случае

$$p^\lambda z^2 \equiv p^\lambda a_1 \pmod{p^\alpha};$$

сокращаем обе части и модуль на p^λ:

$$z^2 \equiv a_1 \pmod{p^{\alpha-\lambda}}. \tag{131a}$$

Если (131) имеет решения, то и (131a) тоже имеет решения, и обратно. Но для разрешимости (131a) необходимо и достаточно, чтобы при p простом нечетном было: $\left(\frac{a_1}{p}\right) = +1$, а при $p = 2$, $\alpha - \lambda > 2$ должно быть: $a_1 \equiv 1 \pmod 8$ (§ 35, теорема 78).

Пусть z — одно из решений сравнения (131a); оно дает бесчисленное множество значений $z + kp^{\alpha-\lambda}$. Все они (при любом целом k) — представители одного и того же решения z (по модулю $p^{\alpha-\lambda}$). Но, умножив эти значения на p^μ, мы найдем решения x сравнения (131); при этом различных по модулю p^α решений будет p^μ, а именно:

$$p^\mu z,\ p^\mu (z + p^{\alpha-\lambda}),\ p^\mu (z + 2p^{\alpha-\lambda}),\ \ldots\ p^\mu [z + (p^\mu - 1)\,p^{\alpha-\lambda}].$$

При других значениях k мы не получим иных (по модулю p^α) решений сравнения (131). Следовательно, всякое решение сравнения (131a) дает p^μ различных (по модулю p^α) решений сравнения (131). Пусть z_1 и z_2 — два различных (по модулю $p^{\alpha-\lambda}$) решения сравнения (131a). Докажем, что ни одно решение сравнения (131), получаемое из z_1, не сравнимо (по модулю p^α) ни с одним решением сравнения (131), получаемым из z_2. Пусть:

$$p^\mu (z_1 + rp^{\alpha-\lambda}) \equiv p^\mu (z_2 + sp^{\alpha-\lambda}) \pmod{p^\alpha}.$$

Сократим все три части на p^{μ}:

$$z_1 + rp^{\alpha-\lambda} \equiv z_2 + sp^{\alpha-\lambda} \pmod{p^{\alpha-\mu}};$$
$$z_1 - z_2 \equiv (s-r)\,p^{\alpha-\lambda} \pmod{p^{\alpha-\mu}}.$$

Но $\alpha - \lambda < \alpha - \mu$, следовательно:

$$z_1 - z_2 \equiv (s-r)\,p^{\alpha-\lambda} \pmod{p^{\alpha-\lambda}},$$

или:

$$z_1 - z_2 \equiv 0 \pmod{p^{\alpha-\lambda}},\quad z_1 \equiv z_2 \pmod{p^{\alpha-\lambda}},$$

т. е. z_1, z_2 не различны по модулю $p^{\alpha-\lambda}$, что́ противоречит условию.

Таким образом, если сравнение (131а) имеет решения, то сравнение (131) имеет $2p^{\frac{\lambda}{2}}$ решений при p нечетном, или $p=2$, $\alpha-\lambda=2$, $4p^{\frac{\lambda}{2}}$ решений при $p=2$, $\alpha-\lambda>2$ и $p^{\frac{\lambda}{2}}$ решений при $p=2$, $\alpha-\lambda=1$.

2) $\lambda = 2\mu+1$ нечетное; из (131) видно, что x должно делиться на $p^{\mu+1}$. Пусть $x = p^{\mu+1}z$; тогда (131) получит вид:

$$p^{2\mu+2}z^2 \equiv p^{2\mu+1}a_1 \pmod{p^{\alpha}}$$

или, сократив на $p^{2\mu+1}$,

$$pz^2 \equiv a_1 \pmod{p^{\alpha-\lambda}}.$$

Но это сравнение не имеет решений, так как a_1 не делится на p, т. е. из него нельзя определить даже z^2 (§ 39, теорема 60). Следовательно, в этом случае и сравнение (131) не имеет решений.

Итак:

Теорема 80. Сравнение (131) при $\lambda<\alpha$ и при a_1, не делящемся на p, имеет решения только при четном λ и при $\left(\frac{a_1}{p}\right)=+1$ (при p — простом нечетном), или при $a_1\equiv 1 \pmod 4$ (при $p=2$, $\alpha-\lambda=2$), или при $a_1 \equiv 1 \pmod 8$ (при $p=2$, $\alpha-\lambda>2$) и всегда при $p=2$, $\alpha-\lambda=1$ (при четном λ). В этих случаях оно имеет: $p^{\frac{\lambda}{2}}$ решений при $p=2$, $\alpha-\lambda=1$; $2p^{\frac{\lambda}{2}}$ решений при p нечетном простом, или при $p=2$, $\alpha-\lambda=2$; $4p^{\frac{\lambda}{2}}$ решений при $p=2$, $\alpha-\lambda>2$.

П р и м е р 1. $x^2\equiv 0 \pmod{81}$; здесь $p=3$, $\alpha=4$ — четное. Получаем решения: 0, 9, 18, 27, 36, 45, 54, 63, 72; всего девять решений, различных по модулю 81.

П р и м е р 2. $x^2\equiv 0 \pmod{128}$; здесь $p=2$, $\alpha=7$ нечетное. Получаем решения: 0, 16, 32, 48, 64, 80, 96, 112; всего восемь решений, различных по модулю 128.

П р и м е р 3. $x^2\equiv 36 \pmod{81}$; здесь $p=3$, $\alpha=4$, $a=36=3^2\cdot 4$; следовательно, $\lambda=2$ — четное; $a_1=4$. Положив $x=3z$, получим для z сравнение $z^2\equiv 4 \pmod 9$; оно, очевидно, имеет решения

$z_1 \equiv 2$, $z_2 \equiv -2 \equiv 7$. Следовательно, получаем такие решения данного сравнения:

$$3 \cdot 2 = 6, \quad 3 \cdot (2+9) = 33, \quad 3 \cdot (2+18) = 60;$$
$$3 \cdot 7 = 21, \quad 3 \cdot (7+9) = 48, \quad 3 \cdot (7+18) = 75;$$

всего шесть решений, различных по модулю 81.

Пример 4. $x^2 \equiv 164 \pmod{512}$; здесь $p = 2$, $\alpha = 9$, $a = 164 = 2^2 \cdot 41$; следовательно, $\lambda = 2$ четное, $a_1 = 41 \equiv 1 \pmod 8$. Положив $x = 2z$, получим для z: $z^2 \equiv 41 \pmod{128}$; имеем: $41 \equiv 9 \pmod{32}$. Таким образом, сравнение $z^2 \equiv 41 \equiv 9 \pmod{32}$ имеет решения: 3, -3, $3 + 16 = 19$, $-3 + 16 = 13$. Из них 19 и 13 удовлетворяют и сравнению $z^2 \equiv 41 \pmod{64}$, а 13 удовлетворяет также сравнению $z^2 \equiv 41 \pmod{128}$. Следовательно, для этого сравнения имеем решения: 13, -13, $13 + 64 = 77$, $-13 + 64 = 51$. А данное сравнение имеет следующие решения:

$$2 \cdot 13 = 26;\ 2 \cdot (13 + 128) = 282;\ 2 \cdot (-13) = -26;\ 2 \cdot (-13 + 128) = 230;\ 2 \cdot 77 = 154;\ 2 \cdot (77 + 128) = 410;\ 2 \cdot 51 = 102;\ 2 \cdot (51 + 128) = 358;$$

всего восемь решений, различных по модулю 512.

Пример 5. $x^2 \equiv 16 \pmod{32}$; здесь $p = 2$, $\alpha = 5$, $a = 16 = 2^4 \cdot 1$; следовательно, $\lambda = 4$ — четное, $a_1 = 1$. При $x = 4z$ получим для z: $z^2 \equiv 1 \pmod 2$; отсюда для z только одно решение: $z \equiv 1$. Решения данного сравнения следующие:

$$4 \cdot 1 = 4;\ 4 \cdot (1 + 2) = 12;\ 4 \cdot (1 + 2 \cdot 2) = 20;\ 4 \cdot (1 + 3 \cdot 2) = 28;$$

всего четыре решения, различных по модулю 32.

§ 57. Рассмотрим теперь сравнение:

$$x^2 \equiv a \pmod m, \qquad (132)$$

где модуль m — какое-нибудь составное (положительное) число. Если $m = p^\alpha q^\beta r^\gamma \ldots$ разложение числа m на простые множители, то по следствию 2 теоремы 68, § 45 сравнение (132) распадается на следующие:

$$\left.\begin{aligned} x^2 &\equiv a \pmod{p^\alpha}, \\ x^2 &\equiv a \pmod{q^\beta}, \\ x^2 &\equiv a \pmod{r^\gamma}, \\ &\ldots\ldots\ldots \end{aligned}\right\} \qquad (133)$$

и имеет решения тогда и только тогда, когда все сравнения (133) имеют решения. При этом число различных по модулю m решений сравнения (132) равно произведению чисел различных по соответствующим модулям решений сравнений (133).

В частности, если m нечетное и a взаимно-простое с m, то сравнения (133) тогда и только тогда имеют решения, когда все символы Лежандра $\left(\frac{a}{p}\right)$, $\left(\frac{a}{q}\right)$, $\left(\frac{a}{r}\right)$, ... равны $+1$; тогда каж-

дое из сравнений (133) имеет два решения. Но тогда символ Якоби

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p}\right)^{\alpha}\left(\frac{a}{q}\right)^{\beta}\left(\frac{a}{r}\right)^{\gamma} \ldots = +1.$$

Это условие необходимо для разрешимости сравнения (132), но недостаточно, ибо из $\left(\frac{a}{m}\right) = +1$ не следует, чтобы все символы $\left(\frac{a}{p}\right)$, $\left(\frac{a}{q}\right)$, $\left(\frac{a}{r}\right)$, ... равнялись $+1$.

Число всех решений (различных по модулю m) сравнения (132) при нечетном m можно представить так:

$$\left[1 + \left(\frac{a}{p}\right)\right]\left[1 + \left(\frac{a}{q}\right)\right]\left[1 + \left(\frac{a}{r}\right)\right] \ldots \qquad (134)$$

Действительно, если хоть один из символов $\left(\frac{a}{p}\right)$, $\left(\frac{a}{q}\right)$, $\left(\frac{a}{r}\right)$, ... равен -1, то соответственный множитель равен нулю; но тогда сравнение (132) не имеет решений (т. е. число решений $= 0$).

Если же все символы $\left(\frac{a}{p}\right)$, $\left(\frac{a}{q}\right)$, $\left(\frac{a}{r}\right)$, ... равны $+1$, то каждый множитель в (134) равен 2. Но тогда каждое из сравнений (133) имеет два решения, а число всех решений сравнения (132) есть 2^{ρ}, где ρ — число различных простых множителей числа m; но то же нам дает и формула (134).

Итак:

Теорема 81. Необходимое (но недостаточное) условие разрешимости сравнения (132) при нечетном m и при a взаимно-простом с m есть: $\left(\frac{a}{m}\right) = +1$. Число различных по модулю m решений сравнения (132) дает выражение (134), где p, q, r, ... — различные простые делители числа m.

Решим несколько общих примеров.

Пример 1. $x^2 \equiv 46 \pmod{105}$. Здесь $105 = 3 \cdot 5 \cdot 7$ — нечетное; $D(46, 105) = 1$.

Данное сравнение распадается на три сравнения:

$$x^2 \equiv 46 \equiv 1 \pmod 3, \quad x^2 \equiv 46 \equiv 1 \pmod 5, \quad x^2 \equiv 46 \equiv 4 \pmod 7.$$

Очевидно, что все они разрешимы; их решения:

$$x \equiv \pm 1 \pmod 3, \quad x \equiv \pm 1 \pmod 5, \quad x \equiv \pm 2 \pmod 7.$$

Эти решения мы комбинируем всеми возможными способами и получаем всего восемь решений данного сравнения.

Возьмем сначала такую комбинацию: $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 7$; первые два сравнения дают: $x \equiv 1 \pmod{15}$, или $x = 1 + 15t$. Подставляя это в третье сравнение, получим: $1 + 15t \equiv 2 \pmod 7$, или $15t \equiv t \equiv 1 \pmod 7$; следовательно, $x \equiv 1 + 15 \cdot 1 \equiv 16 \pmod{105}$; это наше первое решение.

Легко видеть, что комбинация $x \equiv -1 \pmod 3$, $x \equiv -1 \pmod 5$, $x \equiv -2 \pmod 7$ дает решение: $x \equiv -16 \pmod{105}$.

Возьмем теперь комбинацию: $x \equiv 1 \pmod 3$, $x \equiv -1 \pmod 5$, $x \equiv 2 \pmod 7$; первые два сравнения дают: $x = 1 + 3u \equiv -1 \pmod 5$; $3u \equiv -2 \equiv 3 \pmod 5$, $u = 1$, $x \equiv 4 \pmod{15}$, $x = 4 + 15t$. Подставляем это в третье сравнение, получим: $4 + 15t \equiv 2 \pmod 7$, или $t = -2$, $x \equiv 4 - 15 \cdot 2 \equiv -26 \pmod{105}$. Таким образом, третье решение: $x \equiv -26 \pmod{105}$, и сразу же найдем четвертое решение при «противоложной» комбинации: $x \equiv +26 \pmod{105}$.

Теперь берем: $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv -2 \pmod 7$. Первые два сравнения дают: $x \equiv 1 \pmod{15}$; $x = 1 + 15t \equiv -2 \pmod 7$, $t \equiv -3 \pmod 7$; $x \equiv -44 \pmod{105}$; это пятое решение; шестое решение есть: $x \equiv +44 \pmod{105}$.

Теперь берем: $x \equiv 1 \pmod 3$, $x \equiv -1 \pmod 5$, $x \equiv -2 \pmod 7$. Первые два сравнения дают, как мы уже видели, $x \equiv 4 \pmod{15}$; следовательно, $4 + 15t \equiv -2 \pmod 7$, $t \equiv -6 \pmod 7$, или $t \equiv 1 \pmod 7$; следовательно, $x \equiv 19 \pmod{105}$. Это — седьмое решение; а восьмое: $x \equiv -19 \pmod{105}$.

Таким образом, наши восемь решений следующие:

$$\pm 16, \ \pm 19, \ \pm 26, \ \pm 44 \pmod{105}.$$

Пример 2. $x^2 \equiv 17 \pmod{104}$. Здесь $104 = 2^3 \cdot 13$; $D(17, 104) = 1$. Данное сравнение распадается на следующие:

$$x^2 \equiv 17 \equiv 1 \pmod 8; \ x^2 \equiv 17 \equiv 4 \pmod{13}.$$

Оба сравнения разрешимы; решения первого: ± 1, ± 3, второго: ± 2. Имеем опять восемь комбинаций.

Берем: $x \equiv 1 \pmod 8$, $x \equiv 2 \pmod{13}$; это дает: $x = 1 + 8t \equiv 2 \pmod{13}$; $8t \equiv 1 \equiv -12 \pmod{13}$; $2t \equiv -3 \equiv 10 \pmod{13}$, $t \equiv 5 \pmod{13}$; следовательно, $x \equiv 41 \pmod{104}$. Это — первое решение; второе решение: $x \equiv -41 \pmod{104}$.

Теперь берем комбинацию: $x \equiv 1 \pmod 8$, $x \equiv -2 \pmod{13}$; это дает: $x = 1 + 8t \equiv -2 \pmod{13}$; $8t \equiv -3 \equiv -16 \pmod{13}$; $t \equiv -2 \pmod{13}$; следовательно, $x \equiv 1 - 8 \cdot 2 \equiv -15 \pmod{104}$. Это — третье решение, а четвертое: $x \equiv 15 \pmod{104}$.

Теперь берем комбинацию: $x \equiv 3 \pmod 8$, $x \equiv 2 \pmod{13}$; это дает: $x = 3 + 8t \equiv 2 \pmod{13}$; $8t \equiv -1 \equiv 12$; $2t \equiv 3 \equiv -10$; $t \equiv -5 \pmod{13}$; следовательно, $x \equiv 3 - 8 \cdot 5 \equiv -37 \pmod{104}$. Это пятое решение, а шестое; $x \equiv 37 \pmod{104}$.

Наконец, берем: $x \equiv 3 \pmod 8$, $x \equiv -2 \pmod{13}$; это дает: $x = 3 + 8t \equiv -2 \pmod{13}$; $8t \equiv -5 \equiv 8$, $t \equiv 1 \pmod{13}$; следовательно, $x \equiv 11 \pmod{104}$. Это седьмое решение; а восьмое: $x \equiv -11 \pmod{104}$.

Таким образом, восемь решений данного сравнения следующие:

$$\pm 11, \ \pm 15, \ \pm 37, \ \pm 41 \pmod{104}.$$

Пример 3. Решить сравнение $x^2 - 5x + 16 \equiv 0 \pmod{24}$. Помножая все три его части на 4 (§ 46, случай 1), получаем:

$$4x^2 - 20x + 64 \equiv 0 \pmod{96},$$

или:

$$(2x-5)^2 \equiv 25-64 \pmod{96}.$$

Пусть $2x-5=y$, тогда:

$$y^2 \equiv -39 \pmod{96}. \qquad (a)$$

Это сравнение сводится к следующим:

$$y^2 \equiv -39 \equiv -7 \pmod{32}; \quad y^2 \equiv -39 \equiv 0 \pmod{3};$$

первое сравнение имеет четыре решения: 5, —5, $5+16=21$; $-5+16=11$; второе имеет одно решение 0. Следовательно, для решения y сравнения (a) имеем четыре комбинации. Одна из них: $y \equiv 0 \pmod{3}$, $y \equiv 5 \pmod{32}$, или $y=3t \equiv 5 \equiv -27 \pmod{32}$; $t \equiv -9$; следовательно, $y \equiv -27 \pmod{96}$. Это первое решение сравнения (a); второе, очевидно, есть: $y \equiv +27 \pmod{96}$.

Возьмем, далее, комбинацию: $y \equiv 0 \pmod{3}$, $y \equiv 21 \pmod{32}$; находим: $y=3t \equiv 21 \pmod{32}$, т. е. $t \equiv 7$, $y \equiv 21 \pmod{96}$. Это третье решение сравнения (a), а четвертое: $y \equiv -21 \pmod{96}$.

Итак, имеем четыре решения сравнения (a):

$$y \equiv \pm 21, \ \pm 27 \pmod{96}.$$

Каждое из этих значений y подставляем в формулу $2x-5=y$ и каждый раз определяем соответствующее значение x; получаем для x значения: 13, —8, 16, —11. Они все целые, но не все различны по модулю 24, именно: $13 \equiv -11$, $16 \equiv -8 \pmod{24}$. Следовательно, данное сравнение имеет только два решения, различных по модулю 24:

$$x_1 \equiv 13 \pmod{24}, \quad x_2 \equiv 16 \pmod{24}.$$

Пример 4. Решить сравнение $3x^2-16x+12 \equiv 0 \pmod{36}$.

Чтобы свести это сравнение к двучленному, умножим все три его части на 3 (§ 46, случай 2):

$$9x^2-48x+36 \equiv 0 \pmod{108},$$

или:

$$(3x-8)^2 \equiv 64-36 \pmod{108}.$$

Обозначим: $3x-8=y$; тогда:

$$y^2 \equiv 28 \pmod{108}.$$

Это сравнение сводится к следующим:

$$y^2 \equiv 28 \equiv 0 \pmod{4};$$
$$y^2 \equiv 28 \equiv 1 \pmod{27};$$

первое имеет два решения: 0 и 2; второе — тоже два решения: ± 1.

Имеем всего четыре комбинации; берем сначала: $y \equiv 0 \pmod{4}$, $y \equiv 1 \pmod{27}$; это дает: $y=4t \equiv 1 \pmod{27}$; $t=7$, $y \equiv 28 \pmod{108}$. Это — первое решение; второе, очевидно, $y \equiv -28 \pmod{108}$. Далее

берем комбинацию: $y \equiv 2 \pmod 4$, $y \equiv 1 \pmod{27}$; это дает: $y = 2 + 4t \equiv 1 \pmod{27}$; $4t \equiv -1 \pmod{27}$; $t = -7$;

$$y \equiv 2 - 4 \cdot 7 \equiv -26 \pmod{108}.$$

Это — третий корень, а четвертый, очевидно, $y \equiv 26 \pmod{108}$.

Таким образом, для y имеем значения: ± 26, ± 28. Подставляем каждое из них в формулу $3x - 8 = y$ и каждый раз вычисляем x; но значения $y = +26$ и $y = -28$ дают для x дробные значения, которые нам не подходят. Значения же $y = -26$ и $y = +28$ дают: $x = -6$ и $x = +12$,— различные значения по модулю 36. Таким образом, данное сравнение имеет два решения.

Пример 5. Решить сравнение $5x^2 + x + 4 \equiv 0 \pmod{10}$. Чтобы свести его к двучленному, умножим все три его части на $4 \cdot 5 = 20$:

$$100x^2 + 20x + 80 \equiv 0 \pmod{200},$$

или:

$$(10x + 1)^2 \equiv 1 - 80 \pmod{200}.$$

Обозначим: $10x + 1 = y$; тогда:

$$y^2 \equiv -79 \pmod{200}. \qquad \text{(a)}$$

Это сводится на $y^2 \equiv -79 \equiv 1 \pmod 8$; $y^2 \equiv -79 \equiv -4 \pmod{25}$. Первое из этих сравнений дает четыре решения: $y \equiv \pm 1$, ± 3. Чтобы решить второе сравнение, берем сначала:

$$y^2 \equiv -4 \equiv 1 \pmod 5;$$

одно из решений этого сравнения $y \equiv 1$. Берем (§ 54).

$$(1 + \sqrt{-4})^2 = 1 + 2\sqrt{-4} - 4 = -3 + 2\sqrt{-4}.$$

Решим сравнение $-3u \equiv -4 \pmod{25}$, или $3u \equiv -21 \pmod{25}$, $u \equiv -7$. Следовательно, $y \equiv -7 \cdot 2 \equiv -14 \equiv 11 \pmod{25}$. Итак, сравнение $y^2 \equiv -4 \pmod{25}$ имеет решения: ± 11.

Таким образом, мы имеем здесь восемь комбинаций. Берем одну из них: $y \equiv 1 \pmod 8$, $y \equiv 11 \pmod{25}$; следовательно, $y = 1 + 8t \equiv 11 \pmod{25}$, $8t \equiv 10$; $4t \equiv 5 \equiv -20$; $t \equiv -5$; $y \equiv 1 - 8 \cdot 5 \equiv -39 \pmod{200}$. Это одно решение сравнения (a); другое, очевидно, $y \equiv +39 \pmod{200}$.

Теперь берем комбинацию: $y \equiv 1 \pmod 8$, $y \equiv -11 \pmod{25}$; следовательно, $y = 1 + 8t \equiv -11 \pmod{25}$; $8t \equiv -12$; $2t \equiv -3 \equiv 22$, $t \equiv 11$; $y \equiv 1 + 8 \cdot 11 \equiv 89 \pmod{200}$. Это третье решение сравнения (a); четвертое решение есть: $y \equiv -89 \pmod{200}$.

Теперь берем комбинацию: $y \equiv 3 \pmod 8$, $y \equiv 11 \pmod{25}$; следовательно, $y = 3 + 8t \equiv 11 \pmod{25}$; $8t \equiv 8$; $t \equiv 1$; $y \equiv 3 + 8 \cdot 1 \equiv 11 \pmod{200}$. Это пятое решение сравнения (a), а шестое решение: $y \equiv -11 \pmod{200}$.

Наконец, берем комбинацию: $y \equiv 3 \pmod 8$, $y \equiv -11 \pmod{25}$; следовательно, $y = 3 + 8t \equiv -11 \pmod{25}$; $8t \equiv -14$; $4t \equiv -7 \equiv 18$; $2t \equiv 9 \equiv -16$; $t \equiv -8$; $y \equiv 3 - 8 \cdot 8 \equiv -61 \pmod{200}$. Это седьмое

решение сравнения (a), а восьмое решение: $y \equiv +61 \pmod{200}$. Таким образом, имеем восемь решений сравнения (a):

$$\pm 11, \ \pm 39, \ \pm 61, \ \pm 89.$$

Каждое из этих решений подставляем в формулу $10x + 1 = y$ и определяем x. Но значения -11, $+39$, -61, $+89$ дают дробные значения для x, которые не годятся. При $y = +11$, -39, $+61$, -89 получаем: $x = 1$, -4, 6, -9. Но по модулю 10 не все они различны: $1 \equiv -9$, $6 \equiv -4$. Следовательно, имеем только два различных по модулю 10 решения данного сравнения:

$$x_1 \equiv 1 \pmod{10}; \quad x_2 \equiv 6 \pmod{10}.$$

Замечание. Три последних примера можно было бы решить иным способом: вместо того чтобы сначала свести квадратное сравнение к двучленному (по § 46), а затем заменить это двучленное сравнение несколькими сравнениями, модули которых — степени простых чисел (по § 45), можно поступить и наоборот: сначала заменить наше сравнение несколькими сравнениями, модули которых - степени простых чисел, а затем уже каждое из этих сравнений сводить к двучленному. Иногда такой способ более выгодный

Решим этим вторым способом сравнение примера 5:

$$5x^2 + x + 4 \equiv 0 \pmod{10};$$

оно сводится к таким: $5x^2 + x + 4 \equiv 0 \pmod 5$; $5x^2 + x + 4 \equiv 0 \pmod 2$, или, приводя коэффициенты первого по модулю 5, а второго по модулю 2:

$$x - 1 \equiv 0 \pmod 5; \quad x^2 + x = x(x + 1) \equiv 0 \pmod 2.$$

Второе сравнение удовлетворяется всяким числом x, ибо $x(x+1)$ всегда четное; первое же дает $x \equiv 1 \pmod 5$. Следовательно:

1) при $x \equiv 0 \pmod 2$, $x \equiv 1 \pmod 5$ найдем: $x \equiv 6 \pmod{10}$;

2) при $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 5$ найдем: $x \equiv 1 \pmod{10}$.

Мы видим, что в разобранном примере этот способ оказался более простым, чем первый.

УПРАЖНЕНИЯ

71. Сравнение $8x^4 - 9x^3 + 12x^2 - 8 \equiv 0 \pmod{72}$ заменить системой сравнений, модули которых — степени простых чисел (§ 45).

Ответ. $x^2(x - 4) \equiv 0 \pmod 8$; $x^4 - 3x^2 - 1 \equiv 0 \pmod 9$.

72. Привести следующие квадратные сравнения к двучленным: а) $4x^2 - 11x - 3 \equiv 0 \pmod{13}$; б) $5x^2 - 11x + 16 \equiv 0 \pmod{45}$; в) $12x^2 + 8x - 15 \equiv 0 \pmod{44}$ (§ 46).

Ответ. а) $y^2 \equiv 0 \pmod{13}$; $y = x - 3$; б) $y^2 \equiv -16 \pmod{225}$; $y = 5x + 17$; в) $y^2 \equiv 49 \pmod{132}$; $y = 6x + 2$.

73. Пользуясь критерием Эйлера, определить: а) которые из чисел 2, 3, 5 — квадратичные вычеты, которые — невычеты по

модулю 13; б) которые из чисел 5, 7, 8 — квадратичные вычеты, которые — невычеты по модулю 17 (§ 47).

Ответ. а) 2 и 5 — невычеты, 3 — вычет; б) 5 и 7 — невычеты, 8 — вычет.

74. Проверить лемму Гаусса на примере $p = 19$, $a = 5$ (§ 48).

Ответ. $\mu = 4$; $\left(\frac{5}{19}\right) = +1$.

75. Вычислить символы Лежандра: а) $\left(\frac{94}{109}\right)$; б) $\left(\frac{111}{271}\right)$; в) $\left(\frac{342}{677}\right)$; г) $\left(\frac{93}{131}\right)$; д) $\left(\frac{2115}{6269}\right)$; е) $\left(\frac{589}{1283}\right)$ (§ 49).

Ответ. а), в), д), е) $+1$; б), г) -1.

76. Вычислить символы Лежандра и Якоби: а) $\left(\frac{47}{125}\right)$; б) $\left(\frac{5610}{6649}\right)$; в) $\left(\frac{131}{283}\right)$; г) $\left(\frac{116}{397}\right)$; д) $\left(\frac{328}{625}\right)$ (§ 50).

Ответ. а), в) -1; б), г), д) $+1$.

77. Вычислить непосредственно символ Якоби $\left(\frac{521}{825}\right)$, а затем проверить, разложив его на символы Лежандра и вычислив их (§ 50).

Ответ. -1.

78. Найти все квадратичные вычеты числа p: а) $p = 11$; б) $p=13$; в) $p = 17$; г) $p = 19$ (§ 51).

Ответ. а) 1, 3, 4, 5, 9; б) 1, 3, 4, 9, 10, 12; в) 1, 2, 4, 8, 9, 13, 15, 16; г) 1, 4, 5, 6, 7, 9, 11, 16, 17.

79. Доказать, что при $p = 4k+1$ числа a и $p-a$ одновременно квадратичные вычеты или невычеты, а при $p = 4k+3$ из чисел a и $p-a$ одно квадратичный вычет, а другое — невычет (§ 48).

80. Найти все простые делители формы $t^2 - 7u^2$ (§ 51).

Ответ. 2, 7, $28k \pm 1$, $28k \pm 3$, $28k \pm 9$.

81. Найти все простые делители формы $t^2 - 14u^2$ (§ 51).

Ответ. 2, 7, $56k \pm 1$, $56k \pm 5$, $56k \pm 9$, $56k \pm 11$, $56k \pm 13$, $56k \pm 25$.

82. Найти все простые делители формы $t^2 + 5u^2$ (§ 51).

Ответ. 2, 5, $20k + 3$, $20k + 7$, $20k + 9$.

83. Решить сравнения: а) $x^2 \equiv 19 \pmod{31}$; б) $x^2 \equiv 15 \pmod{53}$; в) $x^2 \equiv 11 \pmod{59}$; г) $x^2 \equiv 3 \pmod{37}$ (§ 52).

Ответ. а) $x \equiv \pm 9$; б) $x \equiv \pm 11$; в) решений нет; г) $x \equiv \pm 15$.

84. Решить сравнения: а) $x^2 \equiv 65 \pmod{101}$; б) $x^2 \equiv 7 \pmod{83}$; в) $x^2 \equiv 43 \pmod{109}$ (§ 52).

Ответ. а) $x \equiv \pm 41$; б) $x \equiv \pm 16$; в) $x \equiv \pm 32$.

85. Решить способом Коркина сравнения: а) $x^2 \equiv 11 \pmod{313}$; б) $x^2 \equiv 8 \pmod{641}$ (§ 53).

Ответ. а) $x \equiv \pm 18$; б) $x \equiv \pm 134$.

86. Решить сравнения: а) $x^2 \equiv 24 \pmod{125}$; б) $x^2 \equiv 18 \pmod{343}$; в) $x^2 \equiv 13 \pmod{243}$ (§ 54).

Ответ. а) ± 32; б) ± 19; в) ± 16.

87. Решить сравнения: а) $x^2 \equiv 57 \pmod{512}$; б) $x^2 \equiv 41 \pmod{1024}$; в) $x^2 \equiv 17 \pmod{16384}$ (§ 55).

Ответ. а) ± 85; ± 171; б) ± 205, ± 307; в) ± 1769; ± 6423.

88. Решить сравнения: а) $x^2 \equiv 0 \pmod{625}$, б) $x^2 \equiv 0 \pmod{1331}$ (§ 56).

Ответ. а) 25 решений вида $25k$, где $k = 0, 1, 2, \ldots 24$; б) 11 решений вида $121k$, где $k = 0, 1, 2, \ldots 10$.

89. Решить сравнения: а) $x^2 \equiv 19 \pmod{90}$; б) $x^2 \equiv 98 \pmod{343}$; в) $x^2 \equiv 81 \pmod{729}$; г) $x^2 \equiv 2500 \pmod{3125}$; д) $x^2 \equiv 27 \pmod{243}$; е) $x^2 \equiv 192 \pmod{512}$ (§ 56).

Ответ. а) ± 17; ± 37; б) ± 21, ± 28, ± 70, ± 77, ± 119, ± 126, ± 168; в) ± 9; ± 72, ± 90, ± 153, ± 171, ± 234, ± 252, ± 315, ± 333; г) ± 50; ± 75, ± 175, ± 200, ± 300, ± 325 и т. д., всего 50 решений, учитывая двойные знаки; д) и е) не имеют решений.

90. Решить сравнения: а) $x^2 \equiv 34 \pmod{495}$; б) $x^2 \equiv 48 \pmod{416}$ (§ 57).

Ответ. а) ± 23, ± 32, ± 67, ± 122; б) ± 36, ± 68, ± 140, ± 172.

91. Решить сравнения: а) $8x^2 + 15x - 6 \equiv 0 \pmod{56}$; б) $12x^2 - 11x - 1 \equiv 0 \pmod{30}$.

Ответ. а) 2; 18; б) 1; 7.

92. Решить сравнение: $x^2 + 18x - 18 \equiv 0 \pmod{342}$ (§ 57).

Ответ. 12, —30, 84, —102, 126, —144.

93. Решить сравнение: $x^2 + x + 4 \equiv 0 \pmod{32}$ (§ 57).

Ответ. 12, —13.

94. Решить сравнение: $x^2 + 8x - 20 \equiv 0 \pmod{45}$ (§ 57).

Ответ. 2, 5, 17, 20, 32, 35.

ГЛАВА V

ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

§ 58. В § 37 мы ввели понятие о показателе n, к которому принадлежит данное число a по модулю m; в теореме 59 говорится, что такой показатель n существует для всякого числа a, взаимно-простого с m. Из второго доказательства теоремы Ферма - Эйлера следует:

Теорема 82. Показатели, к которым принадлежат все числа a, взаимно-простые с m, по модулю m, являются делителями числа $\varphi(m)$.

Если теорема Ферма - Эйлера доказана независимо от теоремы 59, то теорема 82 непосредственно следует из теоремы 59 и из теоремы Ферма - Эйлера, ибо в силу последней $a^{\varphi(m)} \equiv a^0 \pmod m$, а вторая часть теоремы 59 говорит, что $\varphi(m) \equiv 0 \pmod n$, т. е. $\varphi(m)$ делится на n.

Как уже было выяснено (§ 37), все степени: $a^0 = 1, a^1, a^2, \ldots$ $\ldots a^{n-1}$ различны по модулю m и являются корнями сравнения:

$$x^n \equiv 1 \pmod m, \tag{135}$$

ибо, очевидно $(a^\lambda)^n = (a^n)^\lambda \equiv 1 \pmod m$.

Определим, к какому показателю принадлежит a^λ по модулю m.

Пусть $(a^\lambda)^k = a^{\lambda k} \equiv 1 \pmod m$; тогда (по теореме 59): $\lambda k \equiv 0 \pmod n$. Обозначим: $D(\lambda, n) = d$; $n = dn_1$, $\lambda = d\lambda_1$; тогда получаем, что $d\lambda_1 k$ делится на dn_1, т. е. $\lambda_1 k$ делится на n_1. Но $D(\lambda_1, n_1) = 1$ (§ 4, теорема 10), следовательно, k делится на n_1 (§ 7, теорема 15), $k = n_1 z$, где z — целое число. С другой стороны: $(a^\lambda)^{n_1} = a^{d\lambda_1 n_1} = a^{\lambda_1 d n_1} = a^{\lambda_1 n} \equiv 1 \pmod m$; это доказывает, что n_1—наименьший показатель, для которого $(a^\lambda)^{n_1} \equiv 1 \pmod m$, т е. n_1 и есть показатель, к которому принадлежит a^λ по модулю m.

Итак:

Теорема 83. Если a принадлежит к показателю n по модулю m, то a^λ принадлежит к показателю $\frac{n}{D(\lambda, n)}$ по тому же модулю.

Следствие 1. a^λ принадлежит по модулю m к тому же самому показателю n, что и a тогда и только тогда, когда λ и n взаимно-простые.

Определение. Корень x сравнения (135) называется *первообразным корнем* этого сравнения, если он принадлежит к показателю n по модулю m.

Из предыдущего следует:

Следствие 2. Если известно, что сравнение (135) имеет один первообразный корень, то оно имеет по крайней мере $\varphi(n)$ первообразных корней.

Из теоремы 82 следует, что сравнение (135) только тогда может иметь первообразные корни, когда n — делитель числа $\varphi(m)$. Но отсюда еще не следует, что для *всякого* делителя n числá $\varphi(m)$ сравнение (135) непременно имеет первообразные корни, т. е. что для *всякого* делителя n числá $\varphi(m)$ существуют числа a, которые принадлежат к показателю n по модулю m.

Среди делителей числа $\varphi(m)$ имеется и само число $\varphi(m)$.

Определение. Первообразные корни сравнения (135) при $n=\varphi(m)$ (если они существуют) называются *первообразными корнями самого числа m*.

Исследуем, у каких чисел существуют первообразные корни. Сначала докажем следующую лемму.

Лемма. Если $a^{\lambda_1}\equiv 1 \pmod{m_1}$, $a^{\lambda_2}\equiv 1 \pmod{m_2}$, ... $a^{\lambda_k}\equiv 1 \pmod{m_k}$, то $a^{\mu}\equiv 1 \pmod{M}$, где $\mu = \mathrm{M}(\lambda_1, \lambda_2, \ldots \lambda_k)$, $M=\mathrm{M}(m_1, m_2, \ldots m_k)$.

Доказательство. Если $a^{\lambda_\alpha}\equiv 1 \pmod{m_\alpha}$, то и $a^{\varkappa\lambda_\alpha}\equiv 1 \pmod{m_\alpha}$ при любом целом положительном $\varkappa$. Следовательно, $a^{\mu}\equiv 1 \pmod{m_\alpha}$ при $\alpha=1, 2, \ldots k$. Но если $a^{\mu}-1$ делится на $m_1, m_2, \ldots m_k$, то $a^{\mu}-1$ делится и на M (по теореме 8, § 3); следовательно, $a^{\mu}\equiv 1 \pmod{M}$.

Пусть теперь $m=p\,q^{\beta}r^{\gamma}\ldots$ разложение m на простые множители. Имеем: $m=\mathrm{M}(p\ , q^{\beta}, r^{\gamma}, \ldots)$; ибо степени $p^{\alpha}, q^{\beta}, r^{\gamma}, \ldots$ попарно взаимно-простые (§ 8, теорема 17).

Если число a взаимно-простое с m, то оно взаимно-простое и с каждой степенью: $p^{\alpha}, q^{\beta}, r^{\gamma}, \ldots$ Пусть a принадлежит к показателю $\varkappa$ по модулю p^{α}, к показателю λ по модулю q^{β}, к показателю μ по модулю r^{γ} и т. д. и пусть $\xi=\mathrm{M}(\varkappa, \lambda, \mu, \ldots)$; тогда в силу доказанной леммы

$$a^{\xi}\equiv 1 \pmod{m}.$$

Если a — первообразный корень числа m, то $\xi=\varphi(m)$. Но, с одной стороны, $\varphi(m)=\varphi(p^{\alpha})\varphi(q^{\beta})\varphi(r^{\gamma})\ldots$ (§ 35, теорема 54, следствие 1); с другой стороны, по теореме 82, $\varkappa$ — делитель числа $\varphi(p^{\alpha})$, λ — делитель числа $\varphi(q^{\beta})$, μ — делитель числа $\varphi(r^{\gamma})$, ... Следовательно, $\varkappa\leq\varphi(p^{\alpha})$, $\lambda\leq\varphi(q^{\beta})$, $\mu\leq\varphi(r^{\gamma})$, ... Если бы только в одной из этих формул имел место знак неравенства, то было бы: $\varkappa\lambda\mu\ldots<\varphi(p^{\alpha})\varphi(q^{\beta})\varphi(r^{\gamma})\ldots$ Но $\xi\leq\varkappa\lambda\mu\ldots$; значит, было бы $\xi<\varphi(m)$. Следовательно, должно быть: $\varkappa=\varphi(p^{\alpha})$, $\lambda=\varphi(q^{\beta})$, $\mu=\varphi(r^{\gamma})$, ..., т. е. a должно быть первообразным корнем и для p^{α}, и для q^{β}, и для r^{γ}, ... Кроме того, должно быть: $\xi=\varkappa\lambda\mu\ldots$, т. е. $\varphi(p^{\alpha})$,

$\varphi(q^\beta)$, $\varphi(r^\gamma)$, ... должны быть попарно взаимно-простыми. Но если p и q — два различных нечетных простых числа, то $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, $\varphi(q^\beta) = q^{\beta-1}(q-1)$ — оба четные, т. е. не взаимно-простые. Следовательно, m не может иметь двух различных нечетных простых делителей, т. е. m должно иметь вид: $m = 2^\rho \cdot p^\alpha$. Но ведь $\varphi(2^\rho) = 2^{\rho-1}$; при $\rho > 1$ $2^{\rho-1}$ — четное и, значит, не взаимно-простое с $\varphi(p^\alpha)$.

Следовательно, первообразные корни у числа m возможны только, если $m = p^\alpha$, или $m = 2p^\alpha$, или $m = 2^\rho$. Но легко выяснить, что в последнем случае должно быть $\rho = 1$ или 2.

Действительно, пусть $\rho > 2$ и a — нечетное, т. е. взаимно-простое с 2^ρ; следовательно, a имеет вид: $a = 4k \pm 1$, и мы имеем:

$$a^{2^{\rho-2}} = 1 \pm 2^\rho k + 2^{\rho+1}N,$$

где N — какое-то целое число, или:

$$a^{2^{\rho-2}} \equiv 1 \pmod{2^\rho}.$$

С другой стороны, $\varphi(2^\rho) = 2^{\rho-1}$, т. е. $2^{\rho-2} = \frac{1}{2}\varphi(2^\rho)$, и для всякого числа a, взаимно-простого с 2^ρ:

$$a^{\frac{1}{2}\varphi(2^\rho)} \equiv 1 \pmod{2^\rho},$$

т. е. первообразных корней для числа 2^ρ не существует.

Таким образом:

Теорема 84. Первообразные корни могут существовать только для чисел: 2, 4, p^α, $2p^\alpha$, где p — нечетное простое число, а α — какой-нибудь целый положительный показатель.

Мы увидим, что для таких чисел первообразные корни действительно существуют.

§ 59. Рассмотрим случай простого нечетного модуля p. Если a принадлежит к показателю n по модулю p, то сравнение

$$x^n \equiv 1 \pmod{p} \qquad (135а)$$

кроме корней $1, a, a^2, \dots a^{n-1}$ не имеет иных корней (по модулю p); это следует из теоремы 64, § 44. Следовательно, если сравнение (135а) имеет хоть один первообразный корень, то оно имеет *точно* $\varphi(n)$ первообразных корней; это — уточнение следствия 2 из теоремы 83 в § 58. В данном случае (по теореме 82) n должно быть делителем числа $\varphi(p) = p - 1$.

Возьмем сравнение:

$$x^{p-1} \equiv 1 \pmod{p}; \qquad (135б)$$

по теореме Ферма - Эйлера это сравнение удовлетворяется всяким числом, не делящимся на p, а следовательно, и всеми корнями сравнений (135а), где n — какой-нибудь делитель числа $p - 1$, т. е. и всеми первообразными корнями этих сравнений.

Но всякое число a, не делящееся на p, т. е. всякий корень сравнения (135б), непременно принадлежит к некоторому показателю n по модулю p, и этот показатель — делитель числа $p-1$.

Найдем все делители d, d', d'', ... числа $p-1$ (включая и единицу и само число $p-1$) и обозначим через $\psi(d)$, $\psi(d')$, $\psi(d'')$, ... количества чисел, принадлежащих к показателям d, d', d'', ... по модулю p. Но мы знаем, что $\psi(d)=\varphi(d)$, или $\psi(d)=0$; то же и для $\psi(d')$, $\psi(d'')$, ... С другой стороны, $\sum\limits_d \psi(d)=p-1$, так как всякое число, не делящееся на p, т. е. всякий корень сравнения (135б), непременно принадлежит по модулю p к показателю d, или d', или d'' ... .

Но по формуле Гаусса (§ 35, теорема 55) $\sum\limits_d \varphi(d)=p-1$, следовательно, $\sum\limits_d \psi(d)=\sum\limits_d \varphi(d)$; здесь каждое слагаемое левой части равно или нулю, или соответствующему слагаемому правой части. Но ведь суммы равны, значит, и соответствующие слагаемые должны быть равны. Следовательно, ни одно из чисел $\psi(d)$ не равно нулю, но при всяком d $\psi(d)=\varphi(d)$. В частности, при $d=p-1$ $\psi(p-1)=$ $=\varphi(p-1)$, или.

Теорема 85. Для всякого нечетного простого числа p существуют первообразные корни; число их $=\varphi(p-1)$.

Практического способа нахождения первообразных корней (т. е., по крайней мере, одного первообразного корня) данного простого числа не существует, приходится просто применять способ испытаний, который можно только немного упорядочить.

§ 60. Рассмотрим теперь случай, когда наш модуль есть степень нечетного простого числа: $m=p^\alpha$; первообразный корень числа p^α — такое число a, взаимно-простое с p^α (т. е. не делящееся на p), которое принадлежит к показателю $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$ по модулю p^α.

Пусть число a принадлежит к показателю n по модулю p; следовательно, $a^n\equiv 1 \pmod p$, т. е. $a^n=1+pN$. Отсюда:

$$a^{np^{\alpha-1}}=(1+pN)^{p^{\alpha-1}}=1+p^\alpha M,$$

где M — целое число, ибо все члены разложения $(1+pN)^{p^{\alpha-1}}$ по формуле бинома Ньютона, начиная со второго, делятся на p^α. Таким образом,

$$a^{np^{\alpha-1}}\equiv 1 \pmod{p^\alpha}.$$

Но при $n<p-1$ ведь $np^{\alpha-1}<p^{\alpha-1}(p-1)=\varphi(p^\alpha)$, т. е. при $n<p-1$ число a не может быть первообразным корнем числа p^α. Следовательно, первообразные корни числа p^α (если они существуют) должны быть первообразными корнями и числа p.

Пусть g — первообразный корень числа p, имеем:

$$g^{p-1}\equiv 1 \pmod p,$$

т. е. $g^{p-1} = 1 + Np$; N — целое число. Рассмотрим случай, когда N не делится на p, т. е. когда $g^{p-1} - 1$, делясь на p, не делится на p^2.

Имеем:

$$g^{p(p-1)} = (1 + Np)^p = 1 + Np^2 + Mp^3,$$

где M — целое число, не делящееся на p (как и N), так как все члены разложения $(1 + Np)^p$ по формуле бинома Ньютона, начиная с третьего, делятся на p^3, а начиная с четвертого, делятся на p^4. Таким образом, можно написать:

$$g^{p(p-1)} = 1 + Lp^2,$$

где L — целое число, не делящееся на p. Возведя обе части последнего равенства снова в степень p, найдем:

$$g^{p^2(p-1)} = (1 + Lp^2)^p = 1 + Lp^3 + Kp^5,$$

где K — целое число; т. е.:

$$g^{p^2(p-1)} = 1 + Hp^3,$$

где H — целое число, не делящееся на p, и т. д. Так, мы найдем общую формулу (методом полной индукции):

$$g^{p^\lambda(p-1)} = 1 + Pp^{\lambda+1}, \qquad (136)$$

где P — целое число, не делящееся на p. Или, иначе:

$$g^{p^\lambda(p-1)} \equiv 1 \pmod{p^{\lambda+1}},$$

но $g^{p^\lambda(p-1)}$ не $\equiv 1 \pmod{p^\mu}$, если $\mu > \lambda + 1$.

Пусть n — показатель, к которому принадлежит g по модулю p^α; следовательно, $g^n \equiv 1 \pmod{p^\alpha}$, а следовательно, и $g^n \equiv 1 \pmod{p}$. Значит, n делится на показатель, к которому принадлежит g по модулю p, т. е. на $p - 1$. С другой стороны, по теореме Ферма-Эйлера $g^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha}$, а следовательно, $p^{\alpha-1}(p-1)$ делится на n. Таким образом, n имеет вид:

$$n = p^t (p - 1),$$

где $0 \leq t \leq \alpha - 1$.

Но если бы было $t < \alpha - 1$, то мы бы имели:

$$g^{p^t(p-1)} \equiv 1 \pmod{p^\alpha},$$

а в силу формулы (136) это сравнение неверно. Следовательно, $t = \alpha - 1$, и g — первообразный корень числа p^α.

Исследуем теперь случай, когда $g^{p-1} - 1$ делится на p^2. Пусть $g^{p-1} - 1 = p^2N$, или $g^{p-1} = 1 + Np^2$; в таком случае найдем:

$$g^{p^{\alpha-2}(p-1)} = (1 + Np^2)^{p^{\alpha-2}} = 1 + Mp^\alpha,$$

где M — целое число; значит:

$$g^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p^\alpha}.$$

Следовательно, g — не первообразный корень числа p^α, так как по модулю p^α он принадлежит к показателю $\leq p^{\alpha-2}(p-1) < \varphi(p^\alpha)$.

Вместе с g все числа вида $f = g + kp$ при любом целом k являются первообразными корнями числа p. Все эти числа сравнимы друг с другом по модулю p. Но по модулю p^α числа f не все сравнимы друг с другом: при $k = 0, 1, 2, \ldots p^{\alpha-1} - 1$ числа $f = g + kp$ различны по модулю p^α, тогда как при других целых значениях k соответствующие значения f будут сравнимыми с теми, которые мы получили при $k = 0, 1, 2, \ldots p^{\alpha-1} - 1$, т. е. несравнимых друг с другом по модулю p^α значений f всего $p^{\alpha-1}$. Исследуем, какие из этих значений f будут первообразными корнями числа p^α. Для этого надо исследовать, в каких случаях $f^{p-1} - 1$, делясь на p, не делится на p^2.

Пусть $g^{p-1} - 1 = N \cdot p$; тогда:

$$f^{p-1} - 1 = (g + kp)^{p-1} - 1 = (g^{p-1} - 1) + p(p-1)kg^{p-2} + Lp^2,$$

где L — целое число, или:

$$f^{p-1} - 1 = Np + p(p-1)kg^{p-2} + Lp^2.$$

Умножим обе части этого равенства на g (g — не делится на p):

$$(f^{p-1} - 1)g = Ngp + p(p-1)kg^{p-1} + Lgp^2;$$

но $g^{p-1} = 1 + Np$, следовательно,

$$(f^{p-1} - 1)g = Ngp + p(p-1)k(Np+1) + Lgp^2,$$

или, иначе:

$$(f^{p-1} - 1)g = (Ng - k)p + Kp^2, \qquad (137)$$

где K — некоторое целое число. Здесь мы различим два случая:

1. N не делится на p (т. е. $g^{p-1} - 1$ не делится на p^2). Для того чтобы правая часть (137) не делилась на p^2, надо, чтобы $u = Ng - k$ не делилось на p; $k = Ng - u$. Пусть u принимает значения меньшие, чем $p^{\alpha-1}$ и не делящиеся на p; число таких значений: $\varphi(p^{\alpha-1}) = p^{\alpha-2}(p-1)$. Найдем для них соответствующие значения k, подставим их в формулу $f = g + kp$ и получим те значения f, которые являются первообразными корнями числа p^α, ибо $f^{p-1} - 1$ для этих значений f не делится на p^2.

2. Пусть теперь N делится на p (т. е. $g^{p-1} - 1$ делится на p^2); в этом случае правая часть (137) не делится на p^2, если только k не делится на p. Следовательно, здесь мы просто даем для k все $\varphi(p^{\alpha-1})$ значений, меньших, чем $p^{\alpha-1}$ и не делящихся на p. Соответствующие значения для f и будут первообразными корнями числа p^α.

Таким образом, в обоих случаях первообразный корень g числа p дает $\varphi(p^{\alpha-1})$ различных по модулю p^α первообразных корней числа p^α. Очевидно, что два различных (по модулю p) первообразных корня g_1 и g_2 числа p дадут и все различные (по модулю p^α) первообразные корни числа p^α, так как $f_1 = g_1 + k_1p$

и $f_2 = g_2 + k_2 p$ несравнимы друг с другом даже по модулю p. Таким образом, всего существует

$$\varphi(p-1)\cdot\varphi(p^{\alpha-1}) = \varphi(p^{\alpha-1}(p-1)) = \varphi(\varphi(p^{\alpha})) \qquad (138)$$

различных по модулю p^{α} первообразных корней числа p^{α}, ибо первообразных корней числа p всего $\varphi(p-1)$ и каждый из них дает $\varphi(p^{\alpha-1})$ первообразных корней числа p^{α}; а так как $p-1$ и $p^{\alpha-1}$ взаимно-простые, то можно применить следствие 1 из теоремы 54 (§ 35). Итак:

Теорема 86. Степень p^{α} простого нечетного числа p всегда имеет первообразные корни; их число $\varphi(\varphi(p^{\alpha}))$. Каждый первообразный корень числа p дает $\varphi(p^{\alpha-1})$ различных по модулю p^{α} первообразных корней числа p^{α}. Сам первообразный корень g числа p тогда и только тогда является первообразным корнем числа p^{α}, когда $g^{p-1}-1$, делясь на p, не делится на p^2.

Пример 1. Найти первообразные корни числа 27. Здесь $p=3$, $\alpha=3$, $\varphi(27)=27\cdot\frac{2}{3}=18$, $\varphi(18)=18\cdot\frac{1}{2}\cdot\frac{2}{3}=6$; следовательно, существует шесть первообразных корней числа 27. Далее, $\varphi(p-1)=\varphi(2)=1$, т. е. существует только один первообразный корень числа 3; он $=2$; $p^{\alpha-1}=3^2=9$; $\varphi(9)=9\cdot\frac{2}{3}=6$. Следовательно, этот корень 2 должен дать все шесть корней числа 27. Имеем: $2^2-1=3\cdot 1$, т. е. $N=1$ не делится на 3, и мы здесь имеем случай 1. Для u даем $\varphi(9)=6$ значений <9 и взаимно-простых с 9; это: 1, 2, 4, 5, 7, 8. Соответствующие значения k найдем по формуле $k=Ng-u=2-u$; получим. $k=1$, 0, —2 —3, —5, —6. Наконец, вычислим значения f по формуле $f=g+kp=2+3k$; получим все шесть первообразных корней числа 27:

$$5,\ 2,\ -4\equiv 23,\ -7\equiv 20,\ -13\equiv 14,\ -16\equiv 11.$$

Пример 2. Найти первообразные корни числа 25. Здесь $p=5$, $\alpha=2$, $\varphi(25)=25\cdot\frac{4}{5}=20$, $\varphi(20)=20\cdot\frac{1}{2}\cdot\frac{4}{5}=8$; следовательно, существует восемь первообразных корней числа 25. Каждый первообразный корень числа 5 дает четыре первообразных корня числа 25, ибо $p^{\alpha-1}=5$, $\varphi(5)=4$. Число 5 имеет $\varphi(4)=2$ первообразных корня, именно, 2 и 3. Имеем: $2^4-1=5\cdot 3$; $N=3$ не делится на 5, т. е. здесь у нас случай 1; $k=Ng-u=6-u$; $u=1, 2, 3, 4$; следовательно, $k=5, 4, 3, 2$; $f=g+kp=2+5k$; это дает: $f_1=27\equiv 2$, $f_2=22\equiv -3$, $f_3=17\equiv -8$, $f_4=12$.

Для корня 3 имеем: $3^4-1=5\cdot 16$; $N=16$ не делится на 5, т. е. у нас опять случай 1; $k=Ng-u=48-u$; $u=1, 2, 3, 4$; $k=47$, 46, 45, 44, или по модулю 25: $k=-3, -4, -5, -6$; $f=3+5k$; это дает:

$$f_5=-12\equiv 13,\ f_6=-17\equiv 8,\ f_7=3,\ f_8=-2\equiv 23.$$

§ 61. Рассмотрим теперь случай модуля $m=2p^{\alpha}$, где p — простое нечетное число.

Теорема 87. Нечетное число a, не делящееся на p, принадлежит к одному и тому же показателю как по модулю p^α, так и по модулю $2p^\alpha$.

Доказательство. Пусть $a^n \equiv 1 \pmod{p^\alpha}$, т. е. $a^n - 1$ делится на p^α; но $a^n - 1$ делится и на 2 (ибо разность двух нечетных чисел — четное число), следовательно, $a^n - 1$ делится и на $2p^\alpha$ (по следствию из теоремы 17, § 8). Таким образом, $a^n \equiv 1 \pmod{2p^\alpha}$. Обратно, если $a^n - 1$ делится на $2p^\alpha$, то оно делится и на p^α. Это и доказывает нашу теорему.

Итак, всякий нечетный первообразный корень числа p^α является первообразным корнем и для числа $2p^\alpha$. Это вытекает из того, что $\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha)$, так как $\varphi(2) = 1$ и если $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$, то, следовательно, $a^{\varphi(2p^\alpha)} \equiv 1 \pmod{2p^\alpha}$ (при нечетном a). Если же a — четный первообразный корень числа p^α, то $a + p^\alpha$ — нечетное число, являющееся тоже первообразным корнем числа p^α, а значит, первообразным корнем и числа $2p^\alpha$. Числа a и $a + p^\alpha$ не различны по модулю p^α, но различны по модулю $2p^\alpha$, и одно из этих чисел четное, а другое — нечетное. Следовательно, число первообразных корней числа $2p^\alpha$ такое же, как и число первообразных корней числа p^α, т. е.:

$$\varphi(\varphi(p^\alpha)) = \varphi(\varphi(2p^\alpha)).$$

Пример. Для числа 54 число первообразных корней такое же, как и для числа 27, т. е. 6 (см. пример 1, § 60). Для 27 первообразные корни, как мы видели, 2, 5, 11, 14, 20, 23; следовательно, для числа 54 первообразные корни: $2 + 27 = 29$, 5, 11, $14 + 27 = 41$, $20 + 27 = 47$, 23.

Остается еще рассмотреть случаи модулей 2 и 4.

При $m = 2$ существует только один класс чисел, взаимно-простых с модулем; его представителем можно считать единицу. Единицу можно считать и первообразным корнем числа 2, ибо

$$\varphi(2) = 1, \text{ т. е. } 1^{\varphi(2)} \equiv 1 \pmod 2.$$

При $m = 4$ существует два класса чисел, взаимно-простых с модулем, их представители 1 и 3. Здесь $\varphi(4) = 2$ и $3^{\varphi(4)} \equiv 1 \pmod 4$, следовательно, 3 и является первообразным корнем числа 4, он — единственный (по модулю 4). Но $\varphi(\varphi(4)) = \varphi(2) = 1$, т. е. и здесь число первообразных корней есть $\varphi(\varphi(4))$ подобно тому, как в предыдущих случаях.

Итак:

Теорема 88. Для числа $2p^\alpha$ (p — простое, нечетное) существует $\varphi(\varphi(2p^\alpha))$ первообразных корней; всякий нечетный первообразный корень числа p^α является первообразным корнем и числа $2p^\alpha$.

Теорема 89. Для числа 2 и 4 существуют первообразные корни; число 2 имеет единственный первообразный корень $= 1$; число 4 имеет единственный первообразный корень $= 3$.

Итак, для чисел, для которых, как говорится в теореме 84,

могут существовать первообразные корни, эти первообразные корни *действительно существуют.*

§ 62. Пусть наш модуль m есть одно из чисел, для которых существуют первообразные корни, т. е. $m=2$, или 4, или p^α, или $2p^\alpha$ (p — простое нечетное, α — целое положительное; в частности, $\alpha=1$). Пусть g — один из первообразных корней числа m; следовательно, все степени $g, g^2, g^3, \ldots g^{\varphi(m)}$ различны по модулю m (§ 37 и § 58). Но все они, как и g, взаимно-простые с m, значит, они являются представителями всех $\varphi(m)$ классов чисел по модулю m, взаимно-простых с m. Таким образом, если a — какое-нибудь число, взаимно-простое с m, то существует один и только один показатель α $(1 \leqq \alpha \leqq \varphi(m))$ такой, что:

$$g^\alpha \equiv a \pmod{m}. \tag{139}$$

Можно поставить и такое условие для α: $0 \leqq \alpha \leqq \varphi(m)-1$, ибо $g^{\varphi(m)} \equiv g^0 \equiv 1 \pmod{m}$. Без этих условий показатель α в (139) определен бесконечно-многозначно, так как вместе с α сравнение (139) удовлетворяется и всеми показателями $\alpha+k\varphi(m)$, где k — любое целое число. Вообще, если $g^\alpha \equiv g^\beta \pmod{m}$, то $\alpha \equiv \beta \pmod{\varphi(m)}$, или $\beta=\alpha+k\varphi(m)$ *).

Таким образом, между классами чисел по модулю m, взаимно-простых с m, и между всеми классами чисел по модулю $\varphi(m)$ существует взаимно-однозначное соответствие: если a — представитель класса чисел по модулю m, взаимно-простых с m, а α — представитель соответствующего класса чисел по модулю $\varphi(m)$, то всегда:

$$a \equiv g^\alpha \pmod{m},$$

где g — некоторый, вполне определенный первообразный корень числа m. Число α (и весь класс, к которому принадлежит α по модулю $\varphi(m)$) называется *индексом* числа a (и всего класса по модулю m, к которому принадлежит a). Обозначают:

$$\alpha \equiv \operatorname{ind} a \pmod{\varphi(m)},$$

или, точнее.

$$\alpha \equiv \operatorname{ind}_g a \pmod{\varphi(m)},$$

так как индекс зависит и от взятого за *основание* первообразного корня g.

Теорема 90. Индекс произведения сравним (по модулю $\varphi(m)$) с суммой индексов отдельных множителей **).

Доказательство. Пусть $\operatorname{ind} a \equiv \alpha$, $\operatorname{ind} b \equiv \beta \pmod{\varphi(m)}$; следовательно, $a \equiv g^\alpha$, $b \equiv g^\beta \pmod{m}$. Но тогда $ab \equiv g^{\alpha+\beta} \pmod{m}$,

*) Можно ввести и степени с отрицательными показателями; такая степень $x=g^{-n}$ означает решение сравнения $g^n x \equiv 1 \pmod{m}$; можно проверить, что наши выводы остаются верными и для отрицательных показателей (см. упражнения 99—101 в конце этой главы).

**) Иногда говорят: индекс произведения *равен* сумме индексов отдельных множителей; но это неточно: в системе индексов мы имеем не равенства, а сравнения по модулю $\varphi(m)$.

или:

$$\text{ind}(ab) \equiv \alpha + \beta \equiv \text{ind}\, a + \text{ind}\, b \pmod{\varphi(m)}.$$

Это непосредственно обобщается и на несколько множителей. Если все множители равны, то получаем:

Следствие. Индекс степени (с натуральным показателем) сравним (по модулю $\varphi(m)$) с индексом основания степени, помноженным на показателя степени. Или, в виде формулы:

$$\text{ind}(a^n) \equiv n \cdot \text{ind}\, a \pmod{\varphi(m)}.$$

Теорема 91. Индекс дроби по модулю m: $\frac{b}{a} \pmod{m}$, т. е. индекс решения сравнения: $ax \equiv b \pmod{m}$ (см. упражнение 53 в конце главы III), в частности, индекс обычного частного $\frac{b}{a}$, если b делится на a, сравним (по модулю $\varphi(m)$) с разностью индексов числителя и знаменателя.

Доказательство. Предполагается, конечно, что a и b взаимно-простые с m. Если $ax \equiv b \pmod{m}$, то и x взаимно-простое с m. По теореме 90: $\text{ind}\, a + \text{ind}\, x \equiv \text{ind}\, b \pmod{\varphi(m)}$; следовательно, $\text{ind}\, x \equiv \text{ind}\, b - \text{ind}\, a \pmod{\varphi(m)}$, что и требовалось доказать.

Теорема 92. Индекс единицы всегда сравним с нулем, индекс основания (т. е. самого первообразного корня g) сравним с единицей, индекс числа -1 (или $m-1$) сравним с $\frac{1}{2}\varphi(m)$. Или:

$$\text{ind}\, 1 \equiv 0 \pmod{\varphi(m)};\ \text{ind}\, g \equiv 1 \pmod{\varphi(m)};\ \text{ind}(-1) \equiv$$
$$\equiv \text{ind}(m-1) \equiv \frac{1}{2}\varphi(m) \pmod{\varphi(m)}.$$

Доказательство. Первые два сравнения непосредственно вытекают из следующих: $g^0 \equiv 1 \pmod{m}$, $g^1 \equiv g \pmod{m}$.

Выведем третье сравнение: имеем: $g^{\varphi(m)} \equiv 1 \pmod{m}$, или:

$$g^{\varphi(m)} - 1 = \left(g^{\frac{1}{2}\varphi(m)} - 1\right)\left(g^{\frac{1}{2}\varphi(m)} + 1\right) \equiv 0 \pmod{m}.$$

Если $m = p^\alpha$ (p — простое, нечетное), то оба множителя не могут одновременно делиться на p, так как их разность $= 2$ не делится на p; следовательно, один из этих множителей (и только один) делится на p^α. Но $g^{\frac{1}{2}\varphi(m)} - 1$ не может делиться на p^α, так как g — первообразный корень числа $m = p^\alpha$, т. е. принадлежит к показателю $\varphi(m)$ по модулю p^α; следовательно:

$$g^{\frac{1}{2}\varphi(m)} + 1 \equiv 0 \pmod{p^\alpha},$$

или:

$$g^{\frac{1}{2}\varphi(m)} \equiv -1 \pmod{p^\alpha},$$

а это и показывает, что $\frac{1}{2}\varphi(m) \equiv \text{ind}(-1) \pmod{\varphi(m)}$.

Если $m = 2p^\alpha$, то $g^{\frac{1}{2}\varphi(m)} + 1$ тоже делится на p^α и, кроме того, четное, ибо g — нечетное; следовательно, и здесь третье сравнение верно.

При $m = 4$ проверяем непосредственно:

$$\frac{1}{2}\varphi(4) = 1, \quad g = 3, \quad 3^1 \equiv -1 \pmod 4.$$

Наконец, при $m = 2$ третьего сравнения не имеется, так как здесь $\varphi(2) = 1$, $\frac{1}{2}\varphi(2)$ — не целое.

Теорема 93. За исключением случая, когда $m = 2$, первообразный корень числа m всегда квадратичный невычет для m.

Доказательство. Если a — квадратичный вычет для m, то, следовательно, имеется такое целое число x, что $x^2 \equiv a \pmod m$; x, как и a, взаимно-простое с m. Возводя обе части последнего сравнения в степень $\frac{1}{2}\varphi(m)$, получим:

$$x^{\varphi(m)} \equiv a^{\frac{1}{2}\varphi(m)} \pmod m.$$

Но по теореме Ферма - Эйлера

$$x^{\varphi(m)} \equiv 1 \pmod m,$$

следовательно,

$$a^{\frac{1}{2}\varphi(m)} \equiv 1 \pmod m.$$

Таким образом, a принадлежит к показателю $\leq \frac{1}{2}\varphi(m)$ по модулю m и поэтому не может быть первообразным корнем числа m.

§ 63. Мы видим, что индексы имеют много аналогии с логарифмами; можно сказать, что индексы — это логарифмы по модулю. Они имеют и такие же приложения, как логарифмы, на основе теорем 90—92, а именно, приложения к решению сравнений, как мы покажем на примерах. Для этих приложений необходимо иметь таблицу индексов, составленную для различных модулей, т. е. таблицу, по которой можно было бы для всякого данного числа (класса), взаимно-простого с данным модулем, найти его индекс, и обратно: по данному индексу найти число.

Такие таблицы индексов составлены для простых модулей до 2000; в конце этой книги дается часть этих таблиц (для простых модулей < 100). Для каждого модуля имеется двойная таблица: одна ее часть (под буквою I—Index) дает возможность находить индексы для данных чисел; другая часть (под буквою N — Numerus) позволяет находить числа по данным индексам.

Каждая из таблиц расположена в виде прямоугольника; в заглавной строке стоят цифры 0, 1, 2, ... 9; в заглавном столбце — тоже цифры 0, 1, 2 ... ; сначала (для небольших модулей) их немного. Чтобы найти индекс данного числа, мы ищем десятки этого числа в заглавном столбце, а единицы — в заглавной строке. На

пересечении строки и столбца, идущих от этих десятков и единиц, внутри таблицы и находится искомый индекс данного числа. Аналогично находим и число по данному индексу.

Пример 1. Пусть наш модуль $=67$; найти $\operatorname{ind} 37$; в левой таблице (под буквой I), соответствующей числу 67, ищем в заглавном столбце (слева) цифру 3, а в заглавной строке (сверху) цифру 7. На пересечении строки и столбца, идущих от 3 и 7, имеем число 44; следовательно, $\operatorname{ind} 37 = 44$, или, правильнее: $\operatorname{ind} 37 \equiv 44 \pmod{66}$.

Пример 2. Пусть наш модуль $=73$ и дано: $\operatorname{ind} x = 65$; найти x. В правой таблице (под буквой N), соответствующей числу 73, ищем: в столбце слева 6, в строке сверху 5. На пересечении строки и столбца, которые начинаются этими цифрами 6 и 5, стоит число 39; следовательно, $x = 39$, или, правильнее: $x \equiv 39 \pmod{73}$.

Конечно, в каждой таблице по модулю p имеются только числа $1, 2, \ldots p-1$ и индексы тоже от 1 до $p-1$ (индексы можно было взять от 0 до $p-2$), т. е. и для чисел и для индексов берутся только их наименьшие положительные вычеты. Таким образом, чтобы пользоваться таблицами, надо сначала найти наименьшие положительные вычеты тех чисел, индексы которых мы будем находить по таблицам.

Чтобы составить таблицу индексов для данного простого модуля p, нужно иметь и основание составляемой системы индексов, т. е. тот первообразный корень g числа p, показателями которого и являются наши индексы. Это основание для каждого модуля p указывается в таблицах. Кроме того, в таблицах для каждого модуля даны и все остальные его первообразные корни.

Имея систему индексов по данному модулю с данным основанием, можно всегда переменить основание, т. е. перейти к системе индексов, если за основание взят какой-нибудь другой первообразный корень того же самого модуля. Рассмотрим эту задачу в общем виде. Пусть g и g_1 — два первообразных корня числа m и число a — взаимно-простое с m; пусть:

$$a \equiv g^{\alpha} \equiv g_1^{\alpha_1} \pmod{m} \qquad (140)$$

т. е.:

$$\alpha \equiv \operatorname{ind}_g a \pmod{\varphi(m)}, \quad \alpha_1 \equiv \operatorname{ind}_{g_1} a \pmod{\varphi(m)}.$$

По следствию из теоремы 90 из сравнения (140) найдем.

$$\alpha \equiv \alpha_1 \operatorname{ind}_g g_1 \pmod{\varphi(m)},$$
$$\alpha_1 \equiv \alpha \operatorname{ind}_{g_1} g \pmod{\varphi(m)},$$

или

$$\left.\begin{aligned} \operatorname{ind}_g a &\equiv \operatorname{ind}_{g_1} a \cdot \operatorname{ind}_g g_1 \pmod{\varphi(m)} \\ \operatorname{ind}_{g_1} a &\equiv \operatorname{ind}_g a \cdot \operatorname{ind}_{g_1} g \pmod{\varphi(m)} \end{aligned}\right\} \qquad (141)$$

Первая формула (141) дает возможность перейти от системы с основанием g_1 к системе с основанием g; вторая формула (141) дает переход от системы с основанием g к системе с основанием g_1.

Положив в первой формуле (141) $a = g$ и приняв во внимание, что $\operatorname{ind}_g g \equiv 1$ (теорема 92), получим:

$$\operatorname{ind}_{g_1} g \cdot \operatorname{ind}_g g_1 \equiv 1 \pmod{\varphi(m)}. \qquad (142)$$

Формулы (141) и (142) аналогичны формулам для перехода от одной системы логарифмов к другой (с иным основанием); выражение $\operatorname{ind}_{g_1} g$ или $\operatorname{ind}_g g_1$ аналогично с тем, которое в теории логарифмов называется «модуль».

Пример 3. В таблицах для модуля 59 мы найдем: $\operatorname{ind}_{10} 43 \equiv 13 \pmod{58}$; найти $\operatorname{ind}_6 43$. Для этого найдем по таблицам: $\operatorname{ind}_{10} 6 \equiv 57$; следовательно, по формулам (141)

$$13 \equiv 57 \operatorname{ind}_6 43 \pmod{58}.$$

Решив это сравнение 1-й степени, найдем:

$$\operatorname{ind}_6 43 \equiv -13 \equiv 45 \pmod{58}.$$

Решим еще несколько примеров на применение теории индексов.

Пример 4. Решить сравнение: $36x \equiv 57 \pmod{83}$.

Как при применении логарифмов мы «логарифмируем» данное выражение или обе части данного уравнения, так и здесь мы, можно сказать, «индексируем» данное сравнение, т. е. переходим к соотношению между индексами:

$$\operatorname{ind} 36 + \operatorname{ind} x \equiv \operatorname{ind} 57 \pmod{82}.$$

Из таблицы индексов находим: $\operatorname{ind} 36 = 28$, $\operatorname{ind} 57 = 29$; следовательно,

$$28 + \operatorname{ind} x \equiv 29 \pmod{82},$$

или:

$$\operatorname{ind} x \equiv 29 - 28 \equiv 1 \pmod{82}.$$

Из правой части таблицы (под буквой N) найдем: $x \equiv 50 \pmod{83}$. (50 здесь основание системы индексов; индекс основания равен единице).

Пример 5. $8x \equiv -11 \pmod{37}$; здесь сначала заменяем: $-11 \equiv 26$; т. е.:

$$8x \equiv 26 \pmod{37}.$$

Переходим к индексам:

$$\operatorname{ind} 8 + \operatorname{ind} x \equiv \operatorname{ind} 26 \pmod{36},$$

или:

$$33 + \operatorname{ind} x \equiv 24 \pmod{36}$$
$$\operatorname{ind} x \equiv -9 \equiv 27 \pmod{36},$$
$$x \equiv 31 \pmod{37}.$$

Прежде чем переходить к индексам, мы могли бы сократить обе части сравнения на 2; получили бы:

$$4x \equiv 13 \pmod{37},$$

а отсюда:

$$22 + \operatorname{ind} x \equiv 13 \pmod{36} \text{ и снова: } \operatorname{ind} x \equiv -9 \equiv 27 \pmod{36}.$$

Пример 6. $x^2 \equiv 31 \pmod{43}$; переходим к индексам:

$$2 \operatorname{ind} x \equiv \operatorname{ind} 31 \equiv 32 \pmod{42},$$
$$\operatorname{ind} x \equiv 16 \pmod{21};$$

а по модулю 42 имеем для $\operatorname{ind} x$ два различных значения:

$$\operatorname{ind} x_1 \equiv 16 \pmod{42}, \quad \operatorname{ind} x_2 \equiv 16 + 21 \equiv 37 \pmod{42}.$$

Отсюда:

$$x_1 \equiv 17 \pmod{43}, \quad x_2 \equiv 26 \pmod{43} \text{ —}$$

два решения, причем $26 \equiv -17 \pmod{43}$.

Пример 7. $x^2 \equiv 23 \pmod{47}$, имеем.

$$2 \operatorname{ind} x \equiv \operatorname{ind} 23 \equiv 39 \pmod{46}.$$

Но это сравнение не имеет решений, ибо модуль и коэффициент при неизвестном делятся на 2, тогда как свободный член 39 не делится на 2 (§ 39, теорема 60). Следовательно, и данное квадратное сравнение не имеет решений, т. е. 23 — квадратичный невычет по модулю 47. Проверим это, вычислив символ Лежандра:

$$\left(\frac{23}{47}\right) = -\left(\frac{47}{23}\right) = -\left(\frac{1}{23}\right) = -1.$$

§ 64. При помощи индексов легко решить всякое двучленное сравнение n-й степени (в частности, квадратное) или доказать, что данное сравнение не имеет решений. Исследуем это в общем случае.

Дано сравнение:

$$x^n \equiv a \pmod{m}; \tag{143}$$

мы считаем, что m имеет первообразные корни и a — взаимно-простое с m. Переходим к индексам:

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\varphi(m)}.$$

Пусть $D(n, \varphi(m)) = d$; необходимое и достаточное условие разрешимости этого сравнения состоит в том, чтобы $\operatorname{ind} a$ делился на d: $\operatorname{ind} a = kd$. В таком случае можно сократить на d все три части нашего сравнения:

$$\frac{n}{d} \operatorname{ind} x \equiv \frac{\operatorname{ind} a}{d} \equiv k \left(\operatorname{mod} \frac{\varphi(m)}{d}\right).$$

Это сравнение имеет одно и только одно решение по модулю $\frac{\varphi(m)}{d}$; но по модулю $\varphi(m)$ оно имеет d различных решений $\operatorname{ind} x$, а сравнение (143) имеет d различных по модулю m решений x. Мы имеем:

$$g^{\operatorname{ind} a} \equiv g^{kd} \equiv a \pmod{m},$$

если g — основание нашей системы индексов. Возвысив обе части этого сравнения в степень $\frac{\varphi(m)}{d}$, получим:

$$g^{k\varphi(m)} \equiv a^{\frac{\varphi(m)}{d}} \pmod{m}.$$

Но по теореме Ферма-Эйлера левая часть сравнима с 1, следовательно,

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m. \qquad (144)$$

Обратно, пусть теперь выполнено условие (144); имеем:

$$g^{\operatorname{ind} a} \equiv a \pmod m.$$

Возводим обе части в степень $\frac{\varphi(m)}{d}$; на основании (144) получим:

$$g^{\frac{\varphi(m)}{d} \operatorname{ind} a} \equiv 1 \pmod m;$$

следовательно, $\frac{\varphi(m)}{d} \operatorname{ind} a$ делится на $\varphi(m)$, т. е. $\operatorname{ind} a$ делится на d, а отсюда следует, что сравнение (143) имеет решения.

Итак:

Теорема 94. Если модуль m имеет первообразные корни, то сравнение (143) n-й степени при $D(m, a) = 1$ имеет решения тогда и только тогда, когда выполнено условие (144), где $d = D(n, \varphi(m))$, при этом d различных по модулю m решений. В частности, при $m = p$ (p — нечетное, простое) условие (144) имеет вид:

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p. \qquad (144a)$$

При $n = 2$ всегда и $d = 2$ (ибо $p - 1$ — четное), и условие (144a) обращается в критерий Эйлера (§ 47, (105)).

Следствие 1. Если $D(n, \varphi(m)) = 1$, то сравнение (143) при всяком a, взаимно-простом с m, имеет одно и только одно решение.

Следствие 2. При всяком основании индексы квадратичных вычетов всегда четные, а индексы квадратичных невычетов — нечетные.

Это следует из доказательства теоремы 94.

Пример 1. $x^5 \equiv 14 \pmod{41}$. Переходим к индексам:

$$5 \operatorname{ind} x \equiv \operatorname{ind} 14 \equiv 25 \pmod{40},$$

или: $\operatorname{ind} x \equiv 5 \pmod 8$.

Следовательно, имеем пять решений:

$$\operatorname{ind} x_1 \equiv 5 \pmod{40}, \quad \operatorname{ind} x_2 \equiv 13 \pmod{40}, \quad \operatorname{ind} x_3 \equiv 21 \pmod{40},$$
$$\operatorname{ind} x_4 \equiv 29 \pmod{40}, \quad \operatorname{ind} x_5 \equiv 37 \pmod{40}$$

отсюда:

$$x_1 \equiv 27, \quad x_2 \equiv 24, \quad x_3 \equiv 35, \quad x_4 \equiv 22, \quad x_5 \equiv 15 \pmod{41}.$$

Условие (144a) здесь имеет вид: $14^8 \equiv 1 \pmod{41}$; оно выполнено.

Пример 2. $x^3 \equiv 42 \pmod{53}$. Здесь: $D(3, 52) = 1$; следовательно, наше сравнение имеет одно и только одно решение. Переходим к индексам:

$$3 \operatorname{ind} x \equiv \operatorname{ind} 42 \equiv 20 \pmod{52};$$

найдем: $\operatorname{ind} x \equiv 24 \pmod{52}$; следовательно,

$$x \equiv 49 \equiv -4 \pmod{53}.$$

Пример 3. $x^6 \equiv 22 \pmod{59}$. Здесь: $D(6,\ 58) = 2$; следовательно, наше сравнение имеет два решения, если только ind 22 — четный. Имеем:

$$6 \operatorname{ind} x \equiv \operatorname{ind} 22 \equiv 12 \pmod{58},$$

или.

$$3 \operatorname{ind} x \equiv 6 \pmod{29},$$
$$\operatorname{ind} x \equiv 2 \pmod{29};$$
$$\operatorname{ind} x_1 \equiv 2 \pmod{58}, \quad \operatorname{ind} x_2 \equiv 31 \pmod{58};$$
$$x_1 \equiv 41 \pmod{59}, \quad x_2 \equiv 18 \pmod{59}.$$

§ 65. Рассмотрим теперь случай модуля $m = 2^\alpha$ при $\alpha > 2$. Мы видели, что всякое нечетное число удовлетворяет сравнению: $a^{\frac{1}{2}\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$; $\frac{1}{2}\varphi(2^\alpha) = 2^{\alpha-2}$. Таким образом, для 2^α не существует первообразных корней. Но мы докажем, что существуют числа, *принадлежащие* к показателю $2^{\alpha-2}$ по модулю 2^α; таким числом, например, является 5.

Имеем: $5 = 1 + 2^2$; $5^2 = 1 + 2^3 + 2^4 \equiv 1 \pmod{2^3}$, но $5^2 \not\equiv 1 \pmod{2^4}$. Далее: $5^{2^2} = (5^2)^2 = 1 + 2^4 + 2^5 + \ldots \equiv 1 \pmod{2^4}$, но $5^{2^2} \not\equiv 1 \pmod{2^5}$.

Пусть доказано, что

$$5^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}, \text{ но } 5^{2^{\lambda-2}} \not\equiv 1 \pmod{2^{\lambda+1}};$$

следовательно,

$$5^{2^{\lambda-2}} = 1 + 2^\lambda k,$$

где k — нечетное число. Тогда:

$$5^{2^{\lambda-1}} = (5^{2^{\lambda-2}})^2 = 1 + 2^{\lambda+1}k + 2^{2\lambda}k^2,$$

а это значит, что

$$5^{2^{\lambda-1}} \equiv 1 \pmod{2^{\lambda+1}}, \text{ но } 5^{2^{\lambda-1}} \not\equiv 1 \pmod{2^{\lambda+2}}.$$

Таким образом, при всяком $\alpha > 2$

$$5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Но при $\nu < \alpha - 2$, $5^{2^\nu} \not\equiv 1 \pmod{2^\alpha}$; это и доказывает, что 5 принадлежит к показателю $2^{\alpha-2}$ по модулю 2^α.

Таким образом, числа $5^0 = 1,\ 5,\ 5^2,\ 5^3, \ldots\ 5^{2^{\alpha-2}-1}$ не сравнимы друг с другом по модулю 2^α. Числа $-1, -5, -5^2, -5^3, \ldots -5^{2^{\alpha-2}-1}$ тоже не сравнимы друг с другом, а также не сравнимы и с числами 5^λ по модулю 2^α, так как числа 5^λ вида $4k + 1$, а числа -5^μ вида $4k + 3$, следовательно, они не сравнимы уже по модулю 4.

Итак, мы имеем $2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(2^\alpha)$ чисел вида:

$$(-1)^\varkappa \cdot 5^\lambda \ (\varkappa = 0,\ 1, \quad \lambda = 0,\ 1,\ 2,\ \ldots\ 2^{\alpha-2} - 1);$$

все они — нечетные, т. е. взаимно-простые с 2^α и различные по модулю 2^α. Следовательно, они — представители всех классов чисел,

взаимно-простых с 2^α (или нечетных). Всякое нечетное число a сравнимо с одним и только с одним произведением $(-1)^\varkappa \cdot 5^\lambda$ с некоторыми $\varkappa$ и λ, определенными $\varkappa$ — по модулю 2, а λ — по модулю $2^{\alpha-2}$.

Таким образом, всякому нечетному числу соответствуют два индекса — $\varkappa$ и λ. Легко проверить, что для этих индексов верны теоремы 90,91 (для каждого индекса отдельно). Можно составить и таблицу индексов (только каждому числу соответствуют два индекса — $\varkappa$ и λ) и пользоваться ею для решения сравнений.

Пример. Пусть модуль $= 2^4 = 16$. Составляем таблицу индексов:

Числа:	1	3	5	7	9	11	13	15
Индексы $\varkappa$:	0	1	0	1	0	1	0	1
Индексы λ:	0	3	1	2	2	1	3	0

Решим сравнение: $5x \equiv 11 \pmod{16}$; переходя к индексам, находим:

для индекса $\varkappa : 0 + \varkappa \equiv 1 \pmod 2$;

для индекса $\lambda : 1 + \lambda \equiv 1 \pmod 4$.

Отсюда: $\varkappa \equiv 1 \pmod 2$, $\lambda \equiv 0 \pmod 4$, а следовательно:

$$x \equiv 15 \equiv -1 \pmod{16}.$$

§ 66. Пусть теперь m — какой-нибудь составной модуль; $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ — его разложение на простые множители. Пусть g_λ — какой-нибудь первообразный корень числа $p_\lambda^{\alpha_\lambda}$ (если p_λ — нечетное; если же $p_1 = 2$ и $\alpha_1 > 2$, то вместо g_1 берем два числа: -1 и 5).

Пусть, далее, a — какое-нибудь число, взаимно-простое с m; в таком случае a — взаимно-простое и с каждым из чисел $p_\lambda^{\alpha_\lambda}$. Следовательно, существует такой показатель ν_λ (определенный по модулю $\varphi(p_\lambda^{\alpha_\lambda})$), что: $a \equiv g_\lambda^{\nu_\lambda} \pmod{p_\lambda^{\alpha_\lambda}}$ (если $p_1 = 2$, $\alpha_1 > 2$, то вместо $g_1^{\nu_1}$ имеем произведение: $(-1)^{\nu_1} \cdot 5^{\nu_1'}$ так, что $a \equiv (-1)^{\nu_1} \cdot 5^{\nu_1'} \pmod{2^{\alpha_1}}$).

Таким образом, мы имеем n таких показателей или «индексов»: $\nu_1, \nu_2, \ldots \nu_n$ (если $p_1 = 2$, $\alpha_1 > 2$, то имеем $n+1$ индексов: $\nu_1, \nu_1', \nu_2, \ldots \nu_n$); они образуют *систему индексов* числа a.

Вместо чисел g_λ возьмем числа a_λ, определяемые следующим образом:

$$a_\lambda \equiv g_\lambda \pmod{p_\lambda^{\alpha_\lambda}}, \quad a_\lambda \equiv 1 \pmod{p_\mu^{\alpha_\mu}} \text{ при } \mu \neq \lambda;$$

каждому g_λ соответствует число a_λ, однозначно определенное по модулю $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = m$ (§ 43, теорема 62, обобщение). И мы имеем (для случая, когда все p_λ нечетные):

$$a \equiv a_1^{\nu_1} a_2^{\nu_2} \ldots a_n^{\nu_n} \pmod m,$$

ибо это дает: $a \equiv g_\lambda^{\nu_\lambda} \pmod{p_\lambda^{\alpha_\lambda}}$, как и должно быть.

Числа $a_1, a_2, \ldots a_n$ образуют *базис* чисел, взаимно-простых с m по модулю m. Всякое число a, взаимно-простое с m, сравнимо по модулю m с произведением вида:

$$a_1^{\nu_1} a_2^{\nu_2} \ldots a_n^{\nu_n},$$

где каждое из чисел ν_λ определяется однозначно по соответствующему модулю $\varphi(p_\lambda^{\alpha_\lambda})$.

Давая для ν_λ значения $\nu_\lambda = 0, 1, 2, \ldots \varphi(p_\lambda^{\alpha_\lambda}) - 1$ $(\lambda = 1, 2, \ldots n)$, мы получим $\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_n^{\alpha_n}) = \varphi(m)$ чисел a, взаимнс-простых с m и не сравнимых друг с другом по модулю m, т. е. представителей всех $\varphi(m)$ классов чисел, взаимно-простых с m.

Если $p_1 = 2$, $\alpha_1 = 1$, то просто $g_1 = 1$.

Если $p_1 = 2$, $\alpha_1 = 2$, то $g_1 = 3$.

Если $p_1 = 2$, $\alpha_1 > 2$, то вместо одного g_1 имеем два числа: -1 и 5, как уже было указано. При $p_1 = 2$, $\alpha_1 > 2$ вместо одного числа a_1 мы определяем два числа: $a_1 \equiv -1 \pmod{2^{\alpha_1}}$, $a_1 \equiv 5 \pmod{2^{\alpha_1}}$; $a_1 \equiv a_1' \equiv 1 \pmod{p_\lambda^{\alpha_\lambda}}$ при $\lambda \neq 1$.

Для определенной таким образом системы индексов теоремы 90, 91 остаются верными. Например, если

$$a \equiv a_1^{\nu_1} a_2^{\nu_2} \ldots a_n^{\nu_n} \pmod{m}, \quad b \equiv a_1^{\rho_1} a_2^{\rho_2} \ldots a_n^{\rho_n} \pmod{m},$$

то, очевидно:

$$ab \equiv a_1^{\nu_1+\rho_1} a_2^{\nu_2+\rho_2} \ldots a_n^{\nu_n+\rho_n} \pmod{m};$$

при этом $\nu_\lambda + \rho_\lambda$ можно свести по модулю $\varphi(p_\lambda^{\alpha_\lambda})$.

Здесь тоже можно составить таблицу индексов, только каждому числу (взаимно-простому с m) будут соответствовать n (или $n+1$) индексов. Этой таблицей можно пользоваться при решении двучленных сравнений, если только коэффициенты в них взаимно-простые с m.

Пример. $m = 105 = 3 \cdot 5 \cdot 7$; $\varphi(m) = \varphi(105) = 105 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 48$, т. е. здесь имеется 48 классов чисел, взаимно-простых с 105. Каждое число, взаимно-простое с 105, имеет три индекса — относительно чисел 3, 5, 7.

Берем $g_1, = 2$, $g_2 = 2$, $g_3 = 3$ (первообразные корни чисел 3, 5, 7) и составляем таблицу:

Числа:	1	2	4	8	11	13	16	17	19	22	23
индексы относительно 3	0	1	0	1	1	0	0	1	0	0	1
» » 5	0	1	2	3	0	3	0	1	2	1	3
» » 7	0	2	4	0	4	3	2	1	5	0	2

Числа:	26	29	31	32	34	37	38	41	43	44	46
индексы относительно 3	1	1	0	1	0	0	1	1	0	1	0
» » 5	0	2	0	1	2	1	3	0	3	2	0
» » 7	5	0	1	4	3	2	1	3	0	2	4

Числа:		47	52	53	58	59	61	62	64	67	68	71
индексы относительно	3	1	0	1	0	1	0	1	0	0	1	1
» »	5	1	1	3	3	2	0	1	2	1	3	0
» »	7	5	1	4	2	1	5	3	0	4	5	0

Числа:		73	74	76	79	82	83	86	88	89	92
индексы относительно	3	0	1	0	0	0	1	1	0	1	1
» »	5	3	2	0	2	1	3	0	3	2	1
» »	7	1	4	3	2	5	3	2	4	5	0

Числа:		94	97	101	103	104
индексы относительно	3	0	0	1	0	1
» »	5	2	1	0	3	2
» »	7	1	3	1	5	3

Найдем еще базис чисел по модулю 105, т. е. определим a_1, a_2, a_3 из следующих сравнений:

$$a_1 \equiv 2 \pmod 3), \quad a_1 \equiv 1 \pmod 5, \quad a_1 \equiv 1 \pmod 7;$$
$$a_2 \equiv 1 \pmod 3, \quad a_2 \equiv 2 \pmod 5, \quad a_2 \equiv 1 \pmod 7;$$
$$a_3 \equiv 1 \pmod 3, \quad a_3 \equiv 1 \pmod 5, \quad a_3 \equiv 3 \pmod 7.$$

Найдем: $a_1 \equiv 71 \pmod{105}$, $a_2 \equiv 22 \pmod{105}$ $a_3 \equiv 31 \pmod{105}$.

Таким образом, всякое число a, взаимно-простое с 105, представляется по модулю 105 в виде

$$a \equiv 71^{\nu_1} \cdot 22^{\nu_2} \cdot 31^{\nu_3} \pmod{105},$$

где $\nu_1 = 0$, или 1; $\nu_2 = 0$, 1, 2, или 3; $\nu_3 = 0$, 1, 2, 3, 4, или 5.

Пользуясь составленной таблицей, решим сравнение:

$$x^2 \equiv 46 \pmod{105}.$$

Обозначим через ν_1, ν_2, ν_3 индексы числа x (относительно 3, 5, 7). Тогда, переходя к индексам,— сначала по модулю 3, а затем по модулю 5, далее по модулю 7,— найдем для ν_1, ν_2, ν_3, следующие сравнения:

$$2\nu_1 \equiv 0 \pmod 2, \quad 2\nu_2 \equiv 0 \pmod 4, \quad 2\nu_3 \equiv 4 \pmod 6.$$

Каждое из этих сравнений имеет два решения:

$$\nu_1 \equiv 0;\ 1; \quad \nu_2 \equiv 0;\ 2; \quad \nu_3 \equiv 2;\ 5.$$

Мы можем комбинировать каждое значение ν_1 с каждым значением ν_2 и с каждым значением ν_3; получим восемь следующих комбинаций индексов:

0, 0, 2; 0, 0, 5; 0, 2, 2; 0, 2, 5; 1, 0, 2;
1, 0, 5; 1, 2, 2; 1, 2, 5.

Для каждой из этих комбинаций найдем в нашей таблице соответствующие значения:

16, 61, 79, 19, 86, 26, 44, 89.

Это — все восемь корней нашего сравнения.

УПРАЖНЕНИЯ

95. Найти показатели, к которым принадлежат по модулю m все числа, взаимно-простые с m, при: а) $m = 5$, б) $m = 8$, в) $m = 10$, г) $m = 11$, д) $m = 24$ (§ 58).

Ответ. а) 2 и 3 — к 4; 4 — к 2; б) 3, 5, 7 — к 2; в) 3 и 7 — к 4; 9 — к 2; г) 2, 6, 7, 8 — к 10; 3, 4, 5, 9 — к 5; 10 — к 2; д) 5, 7, 11, 13, 17, 19, 23 — к 2.

96. Найти все первообразные корни числа: а) 7; б) 17; в) 29; г) 47 (§ 59).

Ответ. а) 3, 5; б) 3, 5, 6, 7, 10, 11, 12, 14; в) 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27; г) 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45.

97. Найти все первообразные корни числа: а) 49; б) 125; в) 121; г) 81 (§ 60).

Ответ. а) 3, 5, 10, 12, 17, 19, 24, 26, 38, 40, 45, 47;

б) 2, 3, 8, 12, 13, 17, 22, 23, 27, 28, 33, 37, 38, 42, 47, 48, 52, 53, 58, 62, 63, 67, 72, 73, 77, 78, 83, 87, 88, 92, 97, 98, 102, 103, 108, 112, 113, 117, 122, 123;

в) 2, 6, 7, 8, 13, 17, 18, 19, 24, 28, 29, 30, 35, 39, 41, 46, 50, 51, 52, 57, 61, 62, 63, 68, 72, 73, 74, 79, 83, 84, 85, 90, 95, 96, 101, 105, 106, 107, 116, 117;

г) 2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77.

98. Найти все первообразные корни числа: а) 14; б) 22; в) 50; г) 162 (§ 61).

Ответ. а) 3, 5; б) 7, 13, 17, 19; в) 3, 13, 17, 23, 27, 33, 37, 47; г) 5, 11, 23, 29, 41, 47, 59, 65, 77, 83, 95, 101, 113, 119, 131, 137, 149, 155.

99. Доказать, что $(a^{-1})^n \equiv (a^n)^{-1} \pmod{m}$, где a — взаимно-простое с m; степени с отрицательными показателями — по модулю m (§ 62).

100. Доказать, что формулы: $a^k \cdot a^l \equiv a^{k+l} \pmod{m}$, $(a^k)^l \equiv$ $\equiv a^{kl} \pmod{m}$ остаются верными и для отрицательных показателей по модулю m (a предполагается взаимно-простым с m) (§ 62).

101. Доказать, что при a взаимно-простом с m $a^\alpha \equiv a^\beta \pmod{m}$ тогда и только тогда, когда $\alpha \equiv \beta \pmod{n}$, где n — показатель, к которому принадлежит a по модулю m, при *любых целых* α *и* β — *положительных или отрицательных* (§ 62).

102. Перестроить таблицу индексов для простого числа 11 (в конце этой книги), взяв за основание первообразный корень 7 (§ 63).

103. Перестроить таблицу индексов для простого числа 19, взяв за основание первообразный корень 2 (§ 63).

104. При помощи индексов решить сравнения: а) $18x \equiv 42 \pmod{89}$; б) $11x \equiv 13 \pmod{31}$; в) $35x + 15 \equiv 0 \pmod{97}$ (§ 63).

Ответ. а) 32; б) 4; в) 55.

105. При помощи индексов решить сравнения: а) $x^2 \equiv 59 \pmod{83}$; б) $x^2 \equiv 32 \pmod{43}$; в) $x^2 \equiv -17 \pmod{53}$; г) $x^2 \equiv 26 \pmod{67}$ (§ 63).

Ответ. а) ± 15; б) нет решений; в) ± 6; г) ± 19.

106. При помощи индексов решить сравнения: а) $x^3 \equiv 15 \pmod{41}$; б) $x^5 \equiv 17 \pmod{29}$; в) $x^7 \equiv 3 \pmod{61}$ (§ 64).

Ответ. а) 7; б) 17, в) 27.

107 При помощи индексов решить сравнения: а) $x^3 \equiv 22 \pmod{43}$; б) $x^6 \equiv 15 \pmod{53}$; в) $x^4 \equiv 11 \pmod{59}$; г) $x^8 \equiv 13 \pmod{23}$; д) $x^8 \equiv 8 \pmod{89}$ (§ 64).

Ответ. а) 19, 28, 39; б) ± 4; в) нет решений; г) ± 9; д) ± 6; ± 17, ± 26, $+ 44$.

108. Составить таблицу индексов для модуля 27, взяв за основание первообразный корень 2; с помощью этой таблицы решить сравнения:

а) $5x \equiv 13 \pmod{27}$; б) $x^2 \equiv 10 \pmod{27}$ (§ 60, 62, 63).

Ответ. а) 8; б) ± 8.

109. Составить таблицу индексов для модуля 50, взяв за основание первообразный корень 3; с помощью этой таблицы решить сравнения:

а) $17x \equiv 39 \pmod{50}$; б) $x^2 \equiv 29 \pmod{50}$ (§ 61, 62, 63).

Ответ. а) 17; б) $+ 23$.

110. Составить таблицу индексов для модуля 24 и найти базис по этому модулю (§ 66).

Ответ. Базис 7, 13, 17.

111. То же самое для модуля 36.

Ответ. Базис 19, 29.

ГЛАВА VI

НЕКОТОРЫЕ СВЕДЕНИЯ О КВАДРАТИЧНЫХ ФОРМАХ

§ 67. *Бинарной квадратичной формой* называется выражение вида

$$\varphi(x, y) = ax^2 + bxy + cy^2,$$

т. е. квадратная однородная функция от двух переменных. В теории чисел рассматриваются такие формы с *целыми* коэффициентами a, b, c, и переменным x, y даются только *целые* значения. Квадратичная форма вполне определяется своими коэффициентами a, b, c; ее сокращенное обозначение:

$$\varphi = (a, b, c).$$

Главная задача теории квадратичных форм — определить, «представляется» ли данное целое число m данной квадратичной формой (a, b, c) и если представляется, то найти все эти «представления» или, иными словами, выяснить, имеет ли неопределенное уравнение

$$ax^2 + bxy + cy^2 = m$$

целые решения x, y и если имеет, то найти все эти целые решения.

В связи с этой основной задачей стоят и дальнейшие задачи: найти все целые числа, которые представляются данной квадратичной формой, и обратно,— найти все квадратичные формы, которыми представляется данное целое число. Эти задачи сводятся к следующей: найти квадратичные формы, представляющие одни и те же числа; такие формы называются *эквивалентными*. Доказывается, что такие и только такие формы могут быть преобразованы друг в друга линейным преобразованием переменных x, y с детерминантом, равным ± 1.

Но теория квадратичных форм не ограничивается указанными задачами; она находится в тесной связи и с теорией квадратных иррациональностей, и с теорией цепных дробей, и даже с теорией эллиптических функций.

Выражение $D = b^2 - 4ac$ называется *дискриминантом* формы (a, b, c). Общий наибольший делитель s коэффициентов a, b, c

данной формы называется *делителем* формы (a, b, c); если $a = sa'$, $b = sb'$, $c = sc'$, то

$$(a, b, c) = s(a', b', c').$$

Форма (a', b', c'), коэффициенты которой взаимно-простые, называется *первообразною*. Очевидно:

$$D = b^2 - 4ac = s^2(b'^2 - 4a'c').$$

Пусть целое число k представляется формой (a, b, c), т. е. существуют такие целые числа α, γ, что

$$a\alpha^2 + b\alpha\gamma + c\gamma^2 = k. \qquad (145)$$

Пусть $D(\alpha, \gamma) = s$; при $s > 1$ представление *несобственное*; если же $s = 1$, т. е. α и γ взаимно-простые, то представление — *собственное*. Пусть $\alpha = s\alpha'$, $\gamma = s\gamma'$; тогда из (145) найдем:

$$k = s^2k'; \quad k' = a\alpha'^2 + b\alpha'\gamma' + c\gamma'^2,$$

и представление числа k' собственное.

Заметим еще, что если форма (a, b, c) не первообразна, и s — ее делитель, то всякое число k, представляемое этой формой, должно делиться на s: $k = sk_1$, и k_1 представляется первообразной формой (a', b', c') (где $a = sa'$, $b = sb'$, $c = sc'$).

Таким образом, достаточно исследовать только первообразные формы и собственные представления чисел такими формами.

§ 68. Разложимые формы. Квадратичная форма (с целыми коэффициентами) называется *разложимой*, если ее можно представить как произведение двух линейных форм тоже с целыми коэффициентами.

Лемма. Если квадратичная форма с целыми коэффициентами представляется как произведение двух линейных форм с *рациональными* коэффициентами, то она — разложима, т. е. представляется как произведение двух линейных форм с *целыми* коэффициентами.

Доказательство. Пусть $\varphi = (a, b, c) = (\alpha'x + \beta'y)(\gamma'x + \delta'y)$, где α', β', γ', δ' — рациональные дроби. Приводим эти дроби к общему знаменателю s *) и умножаем на него обе части нашего равенства:

$$s\varphi = (\alpha x + \beta y)(\gamma x + \delta y),$$

где α, β, γ, δ — целые числа; при этом, сокращая, мы можем достигнуть того, чтобы было: $D(\alpha, \beta, s) = 1$, $D(\gamma, \delta, s) = 1$. Тогда:

$$sa = \alpha\gamma, \ sb = \alpha\delta + \beta\gamma, \ sc = \beta\delta. \qquad (146)$$

Пусть $p > 1$ — простой делитель числа s; первое равенство (146) говорит, что α или γ,— например, α делится на p; третье равенство (146) подобно же говорит, что β или δ делится на p. Но по-

*) Собственно s есть произведение общего знаменателя чисел α', β' на общий знаменатель чисел γ', δ'.

скольку α делится на p, то β не может делиться на p, ибо $D(\alpha, \beta, s) = 1$; следовательно, δ делится на p. Но тогда второе равенство (146) показывает, что $\beta\gamma$ делится на p, что́ неверно, так как ни β, ни γ не делятся на p (γ — не делится на p, ибо $D(\gamma, \delta, s) = 1$). Отсюда следует, что $s = 1$, т. е. $\varphi = (\alpha x + \beta y)(\gamma x + \delta y)$ с целыми $\alpha, \beta, \gamma, \delta$; и лемма доказана.

Теорема 95. Квадратичная форма $\varphi(a, b, c)$ тогда и только тогда разложима, когда ее дискриминант D — точный квадрат.

Доказательство. Пусть $\varphi = (\alpha x + \beta y)(\gamma x + \delta y)$; тогда $a = \alpha\gamma$, $b = \alpha\delta + \beta\gamma$, $c = \beta\delta$; следовательно,

$$D = b^2 - 4ac = (\alpha\delta + \beta\gamma)^2 - 4\alpha\beta\gamma\delta = (\alpha\delta - \beta\gamma)^2.$$

Обратно, пусть $D = \varepsilon^2$ — точный квадрат; при $a \neq 0$ имеем:

$$4a\varphi = 4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - Dy^2 = \\ = [2ax + (b + \varepsilon)y][2ax + (b - \varepsilon)y].$$

Исходя из этого:

$$\varphi = \frac{1}{4a}[2ax + (b + \varepsilon)y][2ax + (b - \varepsilon)y],$$

а отсюда по предыдущей лемме следует, что форма φ разложима.

Если $a = 0$, то $D = b^2$; $\varphi = y(bx + cy)$.

Специальный случай мы имеем, когда квадратичная форма является квадратом линейной формы. Для этого случая мы докажем следующую теорему:

Теорема 96. Квадратичная форма тогда и только тогда есть квадрат линейной формы (помноженный на постоянный множитель), когда ее дискриминант $D = 0$.

Доказательство. Пусть $\varphi = s(\alpha x + \beta y)^2 = s\alpha^2x^2 + 2s\alpha\beta xy + s\beta^2y^2$; тогда:

$$D = 4s^2\alpha^2\beta^2 - 4s\alpha^2 \cdot s\beta^2 = 0.$$

Обратно, пусть теперь $D = 0$; в таком случае по теореме 95 форма φ разложима (ибо 0 — точный квадрат). Пусть

$$\varphi = s(\alpha x + \beta y)(\gamma x + \delta y),$$

причем $D(\alpha, \beta) = 1$ и $D(\gamma, \delta) = 1$; имеем:

$$D = s^2(\alpha\delta - \beta\gamma)^2 = 0;$$

Конечно, $s \neq 0$, следовательно, $\alpha\delta - \beta\gamma = 0$ или:

$$\alpha\delta = \beta\gamma. \qquad (147)$$

Мы считаем, что φ не равна тождественно нулю; следовательно, при $\alpha = 0$ $\beta \neq 0$. Но тогда (147) дает: $\gamma = 0$, и наша форма имеет вид:

$$\varphi = s\beta\delta \cdot y^2.$$

Аналогично, при $\delta = 0$ и $\beta = 0$, и тогда $\varphi = s\alpha\gamma x^2$.

Пусть теперь $\alpha, \beta, \gamma, \delta$ все отличны от нуля; по (147) $\alpha\delta$ делится на γ, но γ и δ взаимно-простые, следовательно, α делится

на γ. Так же из (147) мы найдем, что и γ делится на α, т. е. $\alpha = \pm\gamma$. Мы можем считать α и γ положительными, изменив, если это потребуется, знак у s. Следовательно, $\alpha = \gamma$, а тогда из (147) найдем: $\beta = \delta$, т. е.

$$\varphi = s(\alpha x + \beta y)^2,$$

что́ и требовалось доказать.

Если $\varphi = (\alpha x + \beta y)(\gamma x + \delta y)$ разложимая форма, то при $x : y = \delta : -\gamma$ или при $x : y = \beta : -\alpha$ будет $\varphi = 0$, т. е. уравнение $\varphi = 0$ имеет целые решения x, y, не равные одновременно нулю; например, $x = +\beta$, $y = -\alpha$. Обратно, пусть $\varphi = 0$ при некоторых целых, не равных одновременно нулю, значениях x и y, т. е.:

$$4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - Dy^2 = 0. \qquad (148)$$

При $y = 0$ это дает: $2ax = 0$; но так как тогда $x \neq 0$, то $a = 0$, и форма $\varphi = y(bx + cy)$ разложима. Если же $y \neq 0$, то (148) дает

$$D = \left(\frac{2ax + by}{y}\right)^2,$$

т. е. D — точный квадрат, и, следовательно (по теореме 95), форма φ — разложима.

Итак:

Теорема 97. Квадратичная форма φ тогда и только тогда разложима, когда существуют целые значения x y, не равные одновременно нулю, при которых φ обращается в нуль

Пример 1. $\varphi = 5x^2 - 6xy - 8y^2$ — разложимая форма, так как для нее

$$D = 36 + 4 \cdot 5 \cdot 8 = 196 = 14^2 \text{ — точный квадрат.}$$

Действительно:

$$4 \cdot 5 \cdot \varphi = 100x^2 - 120xy - 160y^2 = (10x - 6y)^2 - (14y)^2 = $$
$$= (10x - 20y)(10x + 8y).$$

Отсюда:

$$\varphi = (x - 2y)(5x + 4y).$$

При $x = 2$, $y = 1$ $\varphi = 0$; подобно же, при $x = -4$, $y = 5$ $\varphi = 0$.

Пример 2. $\varphi = 18x^2 - 24xy + 8y^2$; здесь $D = 24^2 - 4 \cdot 18$ $8 = 0$, следовательно, φ — квадрат (с точностью до постоянного множителя). Действительно:

$$\varphi = 2(3x - 2y)^2.$$

§ 69. Пусть теперь форма $\varphi = (a, b, c)$ с дискриминантом D неразложима. Мы имели формулу:

$$4a\varphi = (2ax + by)^2 - Dy^2. \qquad (149)$$

Различим два случая:

1) $D < 0$; пусть $D = -\Delta$; $\Delta > 0$; тогда (149) имеет вид.

$$4a\varphi = (2ax + by)^2 + \Delta y^2. \qquad (149a)$$

Правая часть (а значит, и левая) этого равенства положительна при всех целых значениях x, y; следовательно, форма φ при всяких целых значениях x, y имеет всегда один и тот же знак,— тот же, чтó и a (и чтó и c, ибо a и c в этом случае имеют одинаковые знаки). Такая форма называется *определенною*,— *положительною* при $a > 0$ и *отрицательною* при $a < 0$.

2) $D > 0$; тогда из (149) имеем:

$$\text{при } x = b,\ y = -2a \quad 4a\varphi = -4Da^2 < 0;$$
$$\text{при } x = a,\ y = 0 \quad 4a\varphi = 4a^4 > 0.$$

Следовательно, такая форма при целых x, y может иметь как положительные, так и отрицательные значения. Такая форма называется *неопределенною*.

Замечание. Разложимые формы — определенные при $D = 0$ и неопределенные при $D \neq 0$.

§ 70. Рассмотрим квадратичную форму вида $x^2 + ay^2$, где a — целое число; при $a > 0$ она определенная положительная, при $a < 0$ она неопределенная. Для x и y мы будем давать целые значения, причем только такие, чтобы x и ay были взаимно-простыми.

Теорема 98. При $D(x, ay) = 1$ всякий простой делитель $p > 2$ формы $x^2 + ay^2$ должен удовлетворять условию $\left(\frac{-a}{p}\right) = +1$.

Доказательство. Теорема 98 непосредственно следует из теоремы 76 в § 51. Но легко ее доказать и непосредственно: если $x^2 + ay^2$ делится на простое число $p > 2$, т. е. $x^2 + ay^2 \equiv 0 \pmod p$, то $x^2 \equiv -ay^2 \pmod p$; следовательно, $-ay^2$ квадратичный вычет числа p, т. е.

$$\left(\frac{-ay^2}{p}\right) = \left(\frac{-a}{p}\right)\left(\frac{y^2}{p}\right) = \left(\frac{-a}{p}\right) = +1,$$

чтó и требовалось доказать.

Пусть $a > 0$ и $a < p$, где $p > 2$ простое; возьмем уравнение:

$$x^2 + ay^2 = p. \tag{150}$$

Теорема 99. Если при названных условиях уравнение (150) разрешимо в целых числах x, y, то x и y взаимно-простые (т. е. решение x, y — собственное), и это решение единственное.

Замечание. Очевидно, что вместе с (x, y) решениями уравнения (150) будут также $(-x, y)$, $(x, -y)$, $(-x, -y)$; эти четыре решения мы считаем за одно решение.

Доказательство. Числа x, y, удовлетворяющие уравнению (150), очевидно, взаимно-простые, так как иначе они должны были бы делиться на p, но тогда $x^2 + ay^2$ было бы $> p$.

Пусть (x_1, y_1) и (x_2, y_2) — два решения уравнения (150), т. е.

$$x_1^2 + ay_1^2 = p, \quad x_2^2 + ay_2^2 = p. \tag{151}$$

Положим сначала $a > 1$. Умножаем обе части первого уравнения (151) на y_2^2, а обе части второго — на y_1^2 и вычитаем почленно.

$$(x_1y_2 - x_2y_1)(x_1y_2 + x_2y_1) = p\left(y_2^2 - y_1^2\right).$$

Отсюда следует, что или $x_1y_2 - x_2y_1$, или $x_1y_2 + x_2y_1$ делится на p; оба эти выражения одновременно не могут делиться на p, так как их сумма $2x_1y_2$ не делится на p.

Перемножив почленно равенства (151), найдем:

$$(x_1x_2 + ay_1y_2)^2 + a(x_1y_2 - x_2y_1)^2 = p^2, \qquad (152)$$

или:

$$(x_1x_2 - ay_1y_2)^2 + a(x_1y_2 + x_2y_1)^2 = p^2. \qquad (152а)$$

1) Пусть $x_1y_2 - x_2y_1$ делится на p; тогда из (152) найдем: $x_1y_2 - x_2y_1 = 0$ (ибо ведь $a > 1$), или:

$$\frac{x_1}{y_1} = \frac{x_2}{y_2}.$$

Но ведь обе дроби несократимы, следовательно, $x_2 = x_1$, $y_2 = y_1$.

2) Пусть теперь $xy_2 + x_2y_1$ делится на p; но $x_1y_2 + x_2y_1 > 0$ (ибо мы можем считать x_1, y_1, x_2, y_2 все положительными); следовательно, $x_1y_2 + x_2y_1 = np$, где $n \geqq 1$; а это по (152а) при $a > 1$ невозможно.

Пусть теперь $a = 1$, т. е. уравнение (150) имеет вид:

$$x^2 + y^2 = p. \qquad (153)$$

Как и при $a > 1$, мы найдем, что или $x_1y_2 - x_2y_1$, или $x_1y_2 + x_2y_1$ делится на p; имеют место и формулы (152), (152а) при $a = 1$. И мы найдем:

1) при $x_1y_2 - x_2y_1$, делящемся на p: $x_1y_2 - x_2y_1 = 0$, $x_2 = x_1$, $y_2 = y_1$;

2) при $x_1y_2 + x_2y_1$, делящемся на p: $x_1y_2 + x_2y_1 = p$. Но тогда по (152а): $x_1x_2 - y_1y_2 = 0$, $\frac{x_1}{y_1} = \frac{y_2}{x_2}$, $x_1 = y_2$, $y_1 = x_2$. Но очевидно, что если (x, y) — решение уравнения (153), то и (y, x) тоже решение того же уравнения. Такие два решения мы не считаем различными, т. е. и здесь по существу имеется только одно решение.

Следствие. Если уравнение (150) разрешимо в целых числах, то $\left(\frac{-a}{p}\right) = +1$.

Это следует из теоремы 98, так как для всякого целого решения (x, y) x и ay взаимно-простые.

§ 71. Переходим теперь к решению (в целых числах) уравнения (150) для некоторых частных значений a. Для этого выведем сначала одну общую теорему. По следствию в конце § 70 необходимое условие разрешимости уравнения (150) есть $\left(\frac{-a}{p}\right) = +1$, т. е. сравнение $t^2 \equiv -a \pmod p$ должно иметь решения. Обозначим че-

рез t то решение, для которого $0 < t < \frac{p}{2}$. Разложим $\frac{t}{p}$ в цепную дробь:

$$\frac{t}{p} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_s}}}$$

и обозначим: $\frac{p_1}{q_1} = \frac{0}{1}$, $\frac{p_2}{q_2} = \frac{1}{a_1}$, ... $\frac{p_{s+1}}{q_{s+1}} = \frac{t}{p}$ — подходящие дроби. Всегда найдутся две таких соседних подходящих дроби $\frac{p_n}{q_n}$ и $\frac{p_{n+1}}{q_{n+1}}$, что:

$$q_n < \sqrt{p}, \quad q_{n+1} > \sqrt{p}.$$

Имеем (см. (39), § 24):

$$\left|\frac{t}{p} - \frac{p_n}{q_n}\right| = \frac{|tq_n - pp_n|}{pq_n} < \frac{1}{q_n q_{n+1}}.$$

Отсюда:

$$(tq_n - pp_n)^2 < \frac{p^2}{q_{n+1}^2} < \frac{p^2}{p} = p;$$

$$(tq_n - pp_n)^2 + aq_n^2 < p + aq_n^2 < p + ap = (a+1)p.$$

Раскрывая скобки в левой части, найдем:

$$(tq_n - pp_n)^2 + aq_n^2 = (t^2 + a)q_n^2 + pN,$$

где N — целое число. Но $t^2 + a$ делится на p, ибо ведь $t^2 \equiv -a \pmod p$; следовательно, вся левая часть последнего неравенства делится на p.

Итак:

Теорема 100. Если t — решение сравнения $t^2 \equiv -a \pmod p$, причем $0 < t < \frac{p}{2}$, и $\frac{p_n}{q_n}$ — та подходящая дробь разложения $\frac{t}{p}$ в цепную дробь, для которой $q_n < \sqrt{p}$, тогда как $q_{n+1} > \sqrt{p}$, то:

$$(tq_n - pp_n)^2 + aq_n^2 < (a+1)p, \tag{154}$$

причем левая часть этого неравенства делится на p.

Разберем теперь частные случаи.

1) $a = 1$; имеем уравнение (153): $x^2 + y^2 = p$. Необходимое условие его разрешимости в целых числах: $\left(\frac{-1}{p}\right) = +1$, т. е. (§ 48, IV) p должно быть вида $4k+1$; t — решение сравнения:

$$t^2 \equiv -1 \pmod p.$$

Формула (154) принимает здесь вид:

$$(tq_n - pp_n)^2 + q_n^2 < 2p.$$

Но левая часть делится на p и отлична от нуля, следовательно она равна p:

$$(tq_n - pp_n)^2 + q_n^2 = p, \qquad (155)$$

и мы получили снова теорему 42; только теперь доказано, что целое решение x, y уравнения (153) — единственное и дан способ, как его найти.

Пример 1. Дано уравнение: $x^2 + y^2 = 53$; здесь $t = 23$;

$$\frac{t}{p} = \frac{23}{53} = \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{2}}}}.$$

Найдем здесь:

$$p_n = p_3 = 3, \ q_n = q_3 = 7$$

и по формуле (155):

$$x = 23 \cdot 7 - 53 \cdot 3 = 2, \ y = 7; \ 2^2 + 7^2 = 53.$$

2) $a = 2$; имеем уравнение: $x^2 + 2y^2 = p$. Необходимое условие его разрешимости в целых числах: $\left(\frac{-2}{p}\right) = +1$, или: $\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = +1$; следовательно, оба символа $\left(\frac{-1}{p}\right)$ и $\left(\frac{2}{p}\right)$ одного знака, т. е. оба равны $+1$ или оба равны -1.

Но $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = +1$, если $p = 4k + 1 = 8l \pm 1$, а $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$, если $p = 4k + 3 = 8l \pm 3$ (§ 48, IV, V); следовательно, p должно быть вида $8l + 1$ или $8l + 3$. Это необходимое условие для разрешимости в целых числах нашего сравнения; мы докажем, что оно и достаточно. Формула (154) дает:

$$(tq_n - pp_n)^2 + 2q_n^2 < 3p,$$

т. е. левая часть (делящаяся на p) равна или p, или $2p$. Если $(tq_n - pp_n)^2 + 2q_n^2 = p$, то наше уравнение решено. Если же $(tq_n - pp_n)^2 + 2q_n^2 = 2p$, то мы заключаем, что $tq_n - pp_n = 2v$ четное число. Но тогда, сокращая на 2, найдем:

$$q_n^2 + 2v^2 = p,$$

т. е. наше уравнение опять решено: $x = q_n$; $y = v$.

Пример 2. Дано уравнение: $x^2 + 2y^2 = 43$; 43 — вида $8l + 3$, следовательно, наше уравнение имеет целочисленное решение. Для t имеем сравнение: $t^2 \equiv -2 \pmod{43}$; найдем $t = 16$ и, разлагая $\frac{t}{p} = \frac{16}{43}$ в цепную дробь, получим. $p_n = 1$, $q_n = 3$. Далее: $tq_n - pp_n = 5$; $5^2 + 2 \cdot 3^2 = 43$, т. е. решение: $x = 5$, $y = 3$.

3) $a = 3$; наше уравнение: $x^2 + 3y^2 = p$. Необходимое условие

его разрешимости в целых числах: $\left(\frac{-3}{p}\right)=+1$. Но (по закону взаимности и по § 48, IV)

$$\left(\frac{-3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}=\left(\frac{p}{3}\right);$$

$\left(\frac{p}{3}\right)=+1$ при $p=3k+1$, а так как p нечетное, то это равносильно тому, что p вида $6k+1$. Докажем, что это условие и достаточно для целочисленной разрешимости нашего уравнения. Формула (154) дает:

$$(tq_n-pp_n)^2+3q_n^2<4p,$$

т. е. левая часть (делящаяся на p) равна p, $2p$ или $3p$. Обозначим: $tq_n-pp_n=\lambda$.

Если $\lambda^2+3q_n^2=p$, то наше уравнение решено.

Случай $\lambda^2+3q_n^2=2p$ невозможен: если λ и q_n четные, то $\lambda^2+3q_n^2$ делится на 4; если же λ и q_n нечетные, то $\lambda^2\equiv q_n^2\equiv 1 \pmod 4$ (§ 34, теорема 52). Но тогда $\lambda^2+3q_n^2\equiv 0 \pmod 4$, а $2q$ не делится на 4.

Если $\lambda^2+3q_n^2=3p$, то отсюда следует, что λ делится на 3: $\lambda=3\mu$, следовательно, $9\mu^2+3q_n^2=3p$; $q_n^2+3\mu^2=p$.

Пример 3. Дано уравнение: $x^2+3y^2=37$; 37—вида $6k+1$, т. е. условие разрешимости в целых числах выполнено. Сравнение для t: $t^2\equiv -3 \pmod{37}$; найдем: $t=16$. Раскладывая $\frac{16}{37}$ в цепную дробь, получим: $q_n=2$, $p_n=1$. Далее, $tq_n-pp_n=-5$; $5^2+3\cdot 2^2=37$, следовательно, решение: $x=5$, $y=2$.

Итак, мы доказали следующие теоремы:

Теорема 101. Всякое простое число вида $8k+1$ или $8k+3$ (и только этих видов) может быть представлено в виде суммы квадрата и удвоенного квадрата и только одним образом.

Теорема 102. Всякое простое число вида $6k+1$ (и только этого вида) может быть представлено в виде суммы квадрата и утроенного квадрата и только одним образом.

Эти теоремы, равно как и теорему 42 (§ 31), высказал Ферма; доказал их Эйлер.

§ 72. Сделаем еще некоторые замечания:

В формуле (154) мы взяли тот корень t сравнения $t^2\equiv -a \pmod p$, который $<\frac{p}{2}$. Второй корень этого сравнения (т. е. его наименьший положительный вычет): $p-t>\frac{p}{2}$. Мы могли бы взять его вместо t. Посмотрим, какой будет цепная дробь для $p-t$: если $\frac{t}{p}=\frac{1}{z}$, где $z=a_1+\cfrac{1}{a_2+\cfrac{}{\ddots+\cfrac{1}{a_s}}}$,

то: $$\frac{p-t}{p}=1-\frac{1}{z}=\frac{z-1}{z};$$

или: $\frac{p-t}{p}=\frac{1}{\frac{z}{z-1}}=\frac{1}{1+\frac{1}{z-1}}=\frac{1}{1+\frac{1}{(a_1-1)+\frac{1}{a_2}+\cdots+\frac{1}{a_s}}}.$

Так как $t<\frac{p}{2}$, то $\frac{t}{p}<\frac{1}{2}$, т. е. $a_1-1>0$.

Таким образом, разложение $\frac{p-t}{p}$ в цепную дробь имеет на одно звено больше, чем разложение $\frac{t}{p}$. k-й частный знаменатель разложения $\frac{p-t}{p}$ тот же, что $(k-1)$-й частный знаменатель разложения $\frac{t}{p}$ при $k\geqq 3$. Что касается подходящих дробей, если обозначить через $\frac{p_k}{q_k}$ k-ю подходящую разложения $\frac{t}{p}$, а через $\frac{p'_k}{q'_k}$ k-ю подходящую дробь разложения $\frac{p-t}{p}$, то легко проверить, что:

$$q'_{k+1}=q_k;\ p'_{k+1}=q_k-p_k\ (\text{при } k>1).$$

При обозначениях теоремы 100 (§ 71) мы имеем:

$$q'_{n+1}<\sqrt{p}<q'_{n+2},$$

$(p-t)q'_{n+1}-pp'_{n+1}=-tq'_{n+1}+p(q'_{n+1}-p'_{n+1})=-tq_n+pp_n=$ $=-(tq_n-pp_n)$; следовательно, левая часть формулы (154) не изменится, если вместо корня t возьмем корень $p-t$, т. е. и вся формула (154) останется верной. Таким образом, в разобранных в § 71 случаях, когда $a=1$, 2, 3, мы можем найти единственное решение уравнения (150), взяв вместо корня t корень $p-t$.

§ 73. Поставим теперь вопрос о разрешимости в целых числах уравнения

$$x^2+y^2=m, \tag{156}$$

где m — составное нечетное число. Из теоремы 98 заключаем, что всякий простой делитель p числа m должен удовлетворять условию: $\left(\frac{-1}{p}\right)=+1$, т. е. быть вида $4k+1$. Это условие необходимо для разрешимости в целых числах уравнения (156).

Докажем, что оно и достаточно. Если оно выполнено, то из § 57 следует, что сравнение

$$t^2\equiv-1\ (\mathrm{mod}\ m) \tag{157}$$

имеет решения; число всех различных решений по модулю m есть 2^ρ, где ρ — число различных простых делителей числа m.

Но если не считать существенно различными решения вида t и $-t\equiv m-t$, то мы скажем, что число существенно различных

решений сравнения (157) есть $2^{\rho-1}$. Раскладывая $\frac{t}{m}$ (где t — одно из решений (157)) в цепную дробь и обозначая и здесь через $\frac{p_n}{q_n}$ ту подходящую дробь, для которой $q_n < \sqrt{m}$, тогда как $q_{n+1} \geqq \sqrt{m}$, мы и здесь выведем формулу (155), где только вместо p — составное число m.

$$(tq_n - mp_n)^2 + q_n^2 = m.$$

А это и дает решение уравнения (156).

Пример 1. Дано уравнение $x^2 + y^2 = 1369$. Условие для его разрешимости в целых числах выполнено, так как $1369 = 37^2$, а 37 — вида $4k + 1$. Решаем сравнение $t^2 \equiv -1 \pmod{1369}$, а для этого по способу, изложенному в § 54, решим сравнение $b^2 \equiv -1 \pmod{37}$; получим $b = 6$. Теперь берем:

$$(6 + \sqrt{-1})^2 = 35 + 12\sqrt{-1},$$

решаем сравнение $35u \equiv -1 \pmod{1369}$; получим: $u \equiv 352$. После этого найдем:

$$t \equiv 352 \cdot 12 = 4224 \equiv 117.$$

Разложим $\frac{117}{1369}$ в цепную дробь:

$$\frac{117}{1369} = \cfrac{1}{11 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{11}}}}}}.$$

Вычисляя подходящие дроби, найдем: $q_n = 35$, $p_n = 3$. Далее, найдем:

$tq_n - mp_n = 12$; следовательно, наше решение:

$$x = 12, \quad y = 35.$$

Действительно: $12^2 + 35^2 = 37^2 = 1369$.

Пример 2. Дано уравнение $x^2 + y^2 = 1105$. Условие для его разрешимости в целых числах выполнено, так как $1105 = 5 \cdot 13 \cdot 17$, а все эти простые множители вида $4k + 1$. Решаем сравнение

$$t^2 \equiv -1 \pmod{1105}, \qquad (*)$$

которое сводится к системе (§ 57): $t^2 \equiv -1 \pmod 5$, $t^2 \equiv -1 \pmod{13}$, $t^2 \equiv -1 \pmod{17}$. Решения этих сравнений:

$$t \equiv \pm 2 \pmod 5, \quad t \equiv \pm 5 \pmod{13}, \quad t \equiv \pm 4 \pmod{17}.$$

Комбинируя их всевозможными способами друг с другом, найдем восемь решений сравнения (*):

$$\pm 268, \ \pm 463, \ \pm 47, \ \pm 242.$$

Существенно различных решений четыре, а именно: 268, 463, 47, 242 (здесь $\rho = 3$, следовательно, $4 = 2^{\rho-1}$).

1) Берем $t = 268$; находим: $\frac{268}{1105} = (0, 4, 8, 8, 4)$; $q_n = 33$, $p_n = 8$; $tq_n - mp_n = 4$; следовательно, одно решение: $x = 4$, $y = 33$.

2) При $t = 463$ найдем: $\frac{463}{1105} = (0, 2, 2, 1, 1, 2, 2, 1, 1, 2, 2)$; $q_n = 31$, $p_n = 13$; $tq_n - mp_n = 12$; следовательно, второе решение: $x = 12$, $y = 31$.

3) При $t = 47$ найдем: $\frac{47}{1105} = (0, 23, 1, 1, 23)$; $q_n = 24$, $p_n = 1$; $tq_n - mp_n = 23$; следовательно, третье решение: $x = 23$, $y = 24$.

4) При $t = 242$ найдем: $\frac{242}{1105} = (0, 4, 1, 1, 3, 3, 1, 1, 4)$; $q_n = 32$, $p_n = 7$; $tq_n - mp_n = 9$; следовательно, четвертое решение: $x = 9$, $y = 32$.

Можно было бы доказать и в общем случае, что найденные $2^{\rho-1}$ (в нашем случае 4) решений различны и иных решений не существует.

Итак:

Теорема 103. Нечетное число $m > 0$ тогда и только тогда собственно представляется в виде суммы двух взаимно-простых квадратов, когда оно делится только на простые числа вида $4k+1$. Если ρ — число различных таких простых делителей m, то число различных представлений m в виде суммы двух квадратов есть $2^{\rho-1}$.

Рассмотрим теперь уравнение (156) при четном m. Пусть оно имеет собственное решение (т. е. x и y — взаимно-простые); в таком случае x и y оба нечетны. По теореме 52, § 34 имеем: $x^2 \equiv y^2 \equiv 1 \pmod 8$, $m = x^2 + y^2 \equiv 2 \pmod 8$, т. е. m вида $2m_1$, где m_1 вида $4k+1$, т. е. в виде суммы двух взаимно-простых квадратов могут быть представлены только числа, не делящиеся на 4. Далее, очевидно, что при

$$2m_1 = x^2 + y^2$$

мы получим:

$$m_1 = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2,$$

т. е. и нечетное число m_1 представляется в виде суммы двух квадратов, а для этого оно должно удовлетворять условию теоремы 103. Обратно, если:

$$m_1 = u^2 + v^2,$$

то

$$2m_1 = (u+v)^2 + (u-v)^2.$$

Очевидно, что различным представлениям числа m_1 соответствуют и различные представления числа $2m_1$; и обратно.

Итак:

Теорема 104. Четное число тогда и только тогда собственно представляется в виде суммы двух квадратов, когда оно вида $2m$,

где m — нечетное число, делящееся на простые числа только вида $4k+1$. Число различных представлений числа $2m$ — то же, что и числа m.

Пример. Имеем: $61 = 5^2 + 6^2$; отсюда: $122 = (6+5)^2 + (6-5)^2 = 11^2 + 1^2$.

§ 74. Те сведения из теории чисел, которые излагались в первых пяти главах этой книги, принадлежат к так называемой «мультипликативной» теории чисел *), ибо за основное действие над числами там берется умножение (а также деление, как действие, обратное к умножению), и большинство теорем относится к делимости чисел,— к представлению чисел в виде произведений. Вся теория сравнений по существу рассматривает только более сложные случаи делимости.

В настоящей же, шестой главе рассматриваются представления чисел в виде сумм, т. е. основную роль здесь играет действие сложения; эти вопросы относятся к так называемой «аддитивной» теории чисел **). Эта область теории чисел более сложна и не так закончена, как мультипликативная теория чисел. Конечно, обе области тесно связаны между собой и много теорем относятся одинаково как к той, так и к другой.

Докажем еще одну важную теорему, относящуюся к аддитивной теории чисел. Эта теорема тоже принадлежит Ферма.

Теорема 105. Всякое натуральное число может быть представлено как сумма четырех квадратов.

Доказательство. Возьмем следующее тождество:

$$\begin{vmatrix} a & -b \\ b' & a' \end{vmatrix} \cdot \begin{vmatrix} c & -d \\ d' & c' \end{vmatrix} = \begin{vmatrix} ac+bd & -(a'd-b'c) \\ ad'-bc' & a'c'+b'd' \end{vmatrix};$$

или иначе:

$$(aa'+bb')(cc'+dd') = (ac+bd)(a'c'+b'd') + (ad'-bc')(a'd-b'c). \quad (158)$$

Положим здесь:

$$a = x_0 + ix_1;\ b = x_2 + ix_3;\ c = y_0 - iy_1;\ d = y_2 - iy_3;$$
$$a' = x_0 - ix_1;\ b' = x_2 - ix_3;\ c' = y_0 + iy_1;\ d' = y_2 + iy_3.$$

В таком случае:

$$aa' = x_0^2 + x_1^2,\ bb' = x_2^2 + x_3^2,\ cc' = y_0^2 + y_1^2,\ dd' = y_2^2 + y_3^2,$$

и формула (158) принимает вид:

$$(x_0^2 + x_1^2 + x_2^2 + x_3^2)(y_0^2 + y_1^2 + y_2^2 + y_3^2) = z_0^2 + z_1^2 + z_2^2 + z_3^2, \quad (159)$$

где: $z_0 = x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3$; $z_1 = x_0y_1 - x_1y_0 + x_2y_3 - x_3y_2$;
$z_2 = x_0y_2 - x_2y_0 + x_3y_1 - x_1y_3$; $z_3 = x_0y_3 - x_3y_0 + x_1y_2 - x_2y_1$;
$ac + bd = z_0 - iz_1$; $a'c' + b'd' = z_0 + iz_1$;
$ad' - bc' = z_2 - iz_3$; $a'd - b'c = z_0 + iz_3$.

*) От латинского слова multiplicatio — умножение.
**) От латинского слова additio — сложение.

Формула (159) непосредственно обобщается на произведение нескольких сумм четырех квадратов.

Итак:

Лемма. Произведение нескольких сумм четырех квадратов тоже представляется как сумма четырех квадратов.

Отсюда следует, что достаточно доказать теорему 105 для простого числа p.

При $p = 2$ имеем: $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Пусть $p > 2$, т. е. простое нечетное число. Рассмотрим два случая:

1) p вида $4k + 3$, т. е. $-1 = p - 1$ квадратичный невычет числа p. В таком случае в ряду $1, 2, 3, \ldots, p-1$ обязательно встретятся два соседних числа a и $a + 1$ таких, что a — квадратичный вычет, а $a + 1$ — невычет числа p (ибо ведь первое число 1 — вычет, а последнее $p - 1$ — невычет). Но тогда $(-1)(a+1) = -a-1$ — квадратичный вычет (как произведение двух невычетов). Следовательно, существуют такие целые числа x, y, что:

$$x^2 \equiv a \pmod p, \quad y^2 \equiv -a - 1 \pmod p,$$

причем $0 < x < \frac{p}{2}$, $0 < y < \frac{p}{2}$.

Складывая почленно эти два сравнения, получим:

$$x^2 + y^2 + 1 \equiv 0 \pmod p,$$

т. е.

$$x^2 + y^2 + 1 = pq.$$

При этом:

$$pq = x^2 + y^2 + 1 \leqq 2\left(\frac{p-1}{2}\right)^2 + 1 = \frac{p^2 - 2p + 3}{2} \leqq \frac{p^2 - 2p + p}{2} = \frac{p^2 - p}{2},$$

ибо $p \geqq 3$. Отсюда:

$$q \leqq \frac{p-1}{2}; \quad q < \frac{p}{2}.$$

2) Пусть теперь p вида $4k + 1$, т. е. -1 квадратичный вычет числа p; следовательно, существует такое целое положительное число $x < \frac{p}{2}$, что $x^2 \equiv -1 \pmod p$;

$$\text{или: } x^2 + 1 = pq \leq \left(\frac{p-1}{2}\right)^2 + 1 = \frac{p^2 - 2p + 5}{4} < \frac{2p^2}{4} = p \cdot \frac{p}{2},$$

т. е. и здесь $q < \frac{p}{2}$.

Итак, в случае 1) $pq = 0^2 + x^2 + y^2 + 1$; в случае 2) $pq = 0^2 + 0^2 + x^2 + 1$; в обоих случаях $q < \frac{p}{2}$.

Если $q = 1$, то теорема 105 для числа p доказана.

Пусть $q > 1$; $pq = x_0^2 + x_1^2 + x_2^2 + x_3^2$; x_0, x_1, x_2, x_3 — взаимно-простые (ибо и в случае первом и в случае втором, как мы видели, один из квадратов $= 1$). Возьмем за y_0, y_1, y_2, y_3 абсолютно-наименьшие вычеты чисел x_0, x_1, x_2, x_3 по модулю q, т. е. $y_\lambda \equiv x_\lambda \pmod q$,

$-\frac{q}{2} < y_\lambda \leqq +\frac{q}{2}$ $(\lambda = 0, 1, 2, 3)$. Тогда: $\sum_{\lambda=0}^{3} y_\lambda^2 \equiv \sum_{\lambda=0}^{3} x_\lambda^2 \pmod{q}$, или: $\sum_{\lambda=0}^{3} y_\lambda^2 \equiv pq \equiv 0 \pmod{q}$; следовательно:

$$\sum_{\lambda=0}^{3} y_\lambda^2 = qr; \text{ но } \sum_{\lambda=0}^{3} y_\lambda^2 \leqq 4\left(\frac{q}{2}\right)^2 = q^2, \text{ т. е. } qr \leqq q^2, \ r \leqq q.$$

Если $r = q$, то каждое y_λ должно быть равно своему наибольшему значению, т. е. $\frac{q}{2}$; но тогда, значит, каждое $x_\lambda \equiv y_\lambda = \frac{q}{2} \equiv 0 \left(\mathrm{mod}\, \frac{q}{2}\right)$, т. е. каждое x_λ делится на $\frac{q}{2}$. Но ведь все x_λ взаимно-простые, следовательно, $\frac{q}{2} = 1$, $q = 2$. Следовательно, $x_\lambda \equiv 1 \pmod{2}$, т. е. все x_λ нечетные, и $x_\lambda^2 \equiv 1 \pmod{8}$ (§ 34, теорема 52). Но тогда $\sum_{\lambda=0}^{3} x_\lambda^2 \equiv 4 \equiv 0 \pmod{4}$, т. е. $\sum_{\lambda=0}^{3} x_\lambda^2 = pq = 2p \equiv 0 \pmod{4}$, а это неверно, так как p — нечетное. Следовательно, $r < q$.

Из чисел x_λ, y_λ составляем числа z_λ так, чтобы было согласно доказанной лемме:

$$\sum_{\lambda=0}^{3} x_\lambda^2 \cdot \sum_{\lambda=0}^{3} y_\lambda^2 = \sum_{\lambda=0}^{3} z_\lambda^2 = pq \cdot qr = pq^2r.$$

Но все числа z_λ, делятся на q, так как:

$$z_0 \equiv y_0^2 + y_1^2 + y_2^2 + y_3^2 = qr \equiv 0 \pmod{q},$$
$$z_1 \equiv y_0y_1 - y_1y_0 + y_2y_3 - y_3y_2 \equiv 0 \pmod{q}$$

и подобно же z_2 и z_3.

Пусть $D(z_0, z_1, z_2, z_3) = qd$; $z_\lambda = qdx'_\lambda$ $(\lambda = 0, 1, 2, 3)$;

$$D(x'_0, x'_1, x'_2, x'_3) = 1.$$

Тогда:

$$q^2d^2 \sum_{\lambda=0}^{3} x_\lambda'^2 = pq^2r; \quad \sum_{\lambda=0}^{3} x_\lambda'^2 = \frac{pr}{d^2};$$

pr делится на d^2, но $r < q < \frac{p}{2}$, значит, $d^2 \leqq pr < p^2$, $d < p$.

Так как p простое, то d — взаимно-простое с p; следовательно, r делится на d^2:

$$\frac{r}{d^2} = q' < q;$$

$$\sum_{\lambda=0}^{3} x_\lambda'^2 = pq'.$$

Если $q' = 1$, то теорема 105 доказана. Если $q' > 1$, то, рассуждая так же, найдем:

$$\sum_{\lambda=0}^{3} x_\lambda''^2 = pq''$$

и т. д. Но ряд убывающих натуральных чисел $q > q' > q'' > \ldots$ конечен, т. е. после конечного числа таких шагов мы представим p в виде суммы четырех квадратов. Теорема 105, таким образом, доказана.

УПРАЖНЕНИЯ

112. Найти, разложимы ли формы: а) (4, 5, —9); б) (12, —4, —5); в) (2, 1, —3); г) (3, 10, 3); д) (25, —70, 49) и в случае разложимости разложить формы на линейные множители (§ 68).

Ответ. а) $(4x + 9y)(x - y)$; б) $(2x + y)(6x - 5y)$;
в) $(2x + 3y)(x - y)$; г) $(3x + y)(x + 3y)$; д) $(5x - 7y)^2$.

113. Найти, при каких целых значениях x, y обращаются в нуль формы: а) (4, 5, —9); б) (1, 8, 7); в) (2, 5, —8) (§ 68).

Ответ. а) при $x = y$ и при $x = 9t$, $y = -4t$, где t — произвольное целое число; б) при $x = -y$ и при $x = -7y$; в) только при $x = y = 0$.

114. Представить в виде суммы двух квадратов числа: а) 97; б) 113; в) 157; г) 233 (§ 71).

Ответ. а) $4^2 + 9^2$; б) $7^2 + 8^2$; в) $6^2 + 11^2$; г) $8^2 + 13^2$.

115. Представить в виде суммы квадрата и удвоенного квадрата числа: а) 41; б) 131; в) 193; г) 267 (§ 71).

Ответ. а) $3^2 + 2 \cdot 4^2$; б) $9^2 + 2 \cdot 5^2$; в) $11^2 + 2 \cdot 6^2$; г) $13^2 + 2 \cdot 7^2$.

116. Представить в виде суммы квадрата и утроенного квадрата числа: а) 43; б) 151; в) 157; г) 307 (§ 71).

Ответ. а) $4^2+3 \cdot 3^2$; б) $2^2+3 \cdot 7^2$; в) $7^2 +3 \cdot 6^2$; г) $8^2+3 \cdot 9^2$.

117. Решить в целых числах уравнение $x^2 + y^2 = m$, где $m =$ а) 841; б) 3721; в) 5329; г) 2197; д) 625 (§ 73).

Ответ. а) 20; 21; б) 11; 60; в) 48; 55; г) 9; 46; д) 15; 20.

118. Решить в целых числах уравнение $x^2 + y^2 = m^2$, где $m=$ а) 305; б) 377; в) 629; г) 697 (§ 73).

Ответ. а) 4,17; 7,16; б) 4,19; 11,16; в) 2,25; 10,23; г) 11,24; 16,21.

119. Решить в целых числах уравнение $x^2 + y^2 = 1885$ (§ 73).

Ответ. Четыре решения: 6,43; 11,42; 21,38; 27,34.

120. Эмпирическим путем представить в виде суммы четырех квадратов числа: 126, 374, 593, 1000 (§ 74).

ГЛАВА VII

РАБОТЫ ПО ТЕОРИИ ЧИСЕЛ РУССКИХ И СОВЕТСКИХ МАТЕМАТИКОВ

§ 75. Теория чисел еще в дореволюционной России стояла очень высоко. Исследования русских математиков по теории чисел и результаты, ими полученные, были первостепенной важности. Можно сказать, что в нашей стране теория чисел впервые оформилась (в трудах Эйлера) как наука; в нашей же стране получили свое начало и отдельные отрасли теории чисел — аналитическая, алгебраическая и геометрическая. В Советском Союзе теория чисел развилась еще больше; появилась и новая ее отрасль — теория трансцендентных чисел.

В настоящей главе мы изложим вкратце главнейшие результаты в теории чисел, которые были найдены русскими математиками в дореволюционное время и советскими математиками. Несколько подробнее мы остановимся на исследованиях в теории чисел П. Л. Чебышева.

Начнем наш обзор с трудов Эйлера по теории чисел. Имя Эйлера встречалось уже в предыдущих главах этой книги в связи с важнейшими теоремами и задачами.

Леонард Эйлер (1707—1783), самый гениальный математик XVIII столетия, большую часть своей жизни прожил в нашей стране, был членом Петербургской Академии наук, печатал свои многочисленные научные труды в изданиях нашей Академии; он действительно является основоположником теории чисел. Из 756 работ Эйлера, относящихся ко всем отраслям математики и ее приложений, около сотни относятся к теории чисел. Эти работы Эйлера были переизданы в 1849 г. в двух томах под заглавием «Commentationes arithmeticae collectae» («Собранные арифметические сочинения») на латинском языке, на котором и писал Эйлер.

Содержание этих работ весьма разнообразно. Многие из них посвящены решению в целых числах неопределенных уравнений 2-й, 3-й и 4-й степени. В частности, рассмотренные нами в гл. VI теоремы о представлении чисел в виде сумм двух квадратов, или квадрата и удвоенного квадрата, или квадрата и утроенного

квадрата доказаны Эйлером (высказаны эти теоремы были Ферма в XVII ст.)

Ряд работ Эйлера посвящен простым числам. Эйлер опроверг предположение Ферма о том, что все числа вида $2^{2^n}+1$ (при натуральном n) простые, доказав, что уже при $n=5$ число $2^{2^5}+1$ делится на 641. Эйлер ввел числовую функцию, названную его именем и обозначаемую через $\varphi(m)$. Мы рассматривали ее в гл. III, там же была изложена и так называемая малая теорема Ферма, обобщенная и доказанная Эйлером. Эйлер дал решение в целых числах так называемого уравнения Пелля: $ax^2+1=y^2$. Попутно он дал разложение квадратного корня в цепную дробь и ввел функции, известные под именем «скобок Эйлера» (мы их рассматривали в гл. II).

Целый ряд работ Эйлера посвящен теории квадратичных вычетов простого числа. Он дал критерий для квадратичных вычетов (так называемый «критерий Эйлера» — см. гл. IV, § 47), теоремы о произведении квадратичных вычетов и невычетов, правила сводящиеся к формулам для $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, наконец, он первый высказал (но не доказал) знаменитый квадратичный закон взаимности.

Понятия о первообразных корнях и об индексах тоже даны Эйлером (см. гл. V).

Эйлер доказал невозможность рациональных решений уравнений $x^3+y^3=z^3$, $x^4 \pm y^4=z^2$ и др. (это — частные случаи так называемой великой теоремы Ферма о том, что уравнение $x^n+y^n=z^n$ при натуральном $n>2$ не имеет целых решений).

Наконец, Эйлер первый начал применять методы анализа в исследованиях по теории чисел, и в этом смысле он является основоположником так называемой аналитической теории чисел. Так, в гл. I, §§ 12, 13 мы привели доказательство Эйлера теоремы о бесконечности множества простых чисел и вывели формулу Эйлера (в § 13, теорема 24). Аналитические методы Эйлер применяет и в других местах, например, при выводе интересной формулы:

$$\int n=\int(n-1)+\int(n-2)-\int(n-5)-\int(n-7)+\int(n-12)+ \\ +\int(n-15)-\int(n-22)-\ \dots \qquad (160)$$

где $\int n$ означает сумму всех делителей числа n (см. § 17), а вычитаемые 1, 2, 5, 7, 12, 15, ... содержатся в формуле $\frac{3z^2 \pm z}{2}$, причем многочлен правой части обрывается, когда $n-x$ становится <0. Считается $\int 0=n$.

Например:

$$\int 20=\int 19+\int 18-\int 15-\int 13+\int 8+\int 5=42.$$

Следует отметить еще большое количество разнообразных интересных таблиц, встречающихся в различных работах Эйлера по теории чисел.

§ 76. Пафнутий Львович Чебышев (1821—1894) — величайший математик XIX столетия, учился в Московском университете, в 1847 г. переехал в Петербург, был профессором Петербургского университета, а с 1859 г.— ординарным академиком. Он имеет важные работы во многих областях математики и ее приложений — в теории чисел, в теории вероятностей, в анализе,— является создателем новой отрасли математики — теории апроксимации или наилучшего приближения функций.

В 1849 г. вышла докторская диссертация Чебышева «Теория сравнений»; в своей основной части (первые шесть глав) это учебник элементарного курса теории чисел. Но весьма ценны ее последние главы (7-ая и 8-ая) и дополнения, где изложены результаты исследований самого Чебышева. Последнее (3-е) дополнение: «Об определении числа простых чисел, не превосходящих данной величины»,—представляет собой отдельную научную монографию. Остановимся на нем подробнее.

Заметим, что во 2-м издании своей «Теории чисел» (Théorie des nombres», 1808 г.) Лежандр (во 2-м томе, 4-й части, § 8) приводит формулу, которая с достаточно большой точностью дает число простых чисел, находящихся между единицей и данным пределом x, именно:

$$y = \frac{x}{\ln x - 1{,}08366}. \tag{161}$$

Далее, Лежандр проверяет эту формулу на таблицах простых чисел от 10000 до 10^6 и находит довольно хорошее совпадение значения y в (161) с числом простых чисел, меньших x. Таким образом, Лежандр не доказывает формулы (161), а только эмпирически ее проверяет. Чебышев в вышеуказанном «дополнении» к «теории сравнений» доказал, что формула (161) неверна.

Мы изложим подробно исследования Чебышева.

Теорема I. Если $\varphi(x)$ означает число простых чисел, меньших чем x, n — любое натуральное число, $\rho > 0$, то функция

$$\sum_{x=2}^{\infty}\left[\varphi(x+1) - \varphi(x) - \frac{1}{\ln x}\right]\frac{\ln^n x}{x^{1+\rho}} \; {}^{*)} \tag{162}$$

при ρ, стремящемся к нулю, стремится к конечному пределу.

Доказательство. Докажем сначала, что при $\rho \to 0$ все производные выражений:

$$\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}, \tag{163}$$

$$\ln\rho - \sum \ln\left(1 - \frac{1}{\mu^{1+\rho}}\right), \tag{164}$$

$$\sum \ln\left(1 - \frac{1}{\mu^{1+\rho}}\right) + \sum \frac{1}{\mu^{1+\rho}} \tag{165}$$

---

*) $\ln^n x$ означает $(\ln x)^n$.

по ρ стремятся к конечным пределам. Здесь при суммировании m пробегает все натуральные числа от 2 до ∞, а μ — все простые числа от 2 до ∞.

Имеем: $\frac{e^{-x}}{e^x - 1} = \sum e^{-mx}$ (m пробегает целые числа от 2 до ∞).

Отсюда: $\int\limits_0^\infty \frac{e^{-x}}{e^x - 1} x^\rho \, dx = \sum \int\limits_0^\infty e^{-mx} x^\rho \, dx.$

Но $\int\limits_0^\infty e^{-mx} x^\rho \, dx = \frac{1}{m^{1+\rho}} \int\limits_0^\infty e^{-x} x^\rho \, dx$ (что́ получится если положить $mx = z$),

следовательно,

$$\int\limits_0^\infty \frac{e^{-x}}{e^x - 1} x^\rho \, dx = \sum \frac{1}{m^{1+\rho}} \cdot \int\limits_0^\infty e^{-x} x^\rho \, dx. \tag{166}$$

Далее

$$\int\limits_0^\infty e^{-x} x^{-1+\rho} \, dx = \frac{1}{\rho} \int\limits_0^\infty e^{-x} x^\rho \, dx; \tag{167}$$

это получается, если применить формулу интегрирования по частям, положив $u = e^{-x}$, $dv = x^{-1+\rho} \, dx$, следовательно, $v = \frac{x^\rho}{\rho}$, и приняв во внимание, что $\left| \frac{1}{\rho} e^{-x} x^\rho \right|_0^\infty = 0$.

Вычитаем почленно равенства (166) и (167); получаем

$$\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho} = \frac{\int\limits_0^\infty \left(\frac{1}{e^x - 1} - \frac{1}{x} \right) e^{-x} x^\rho \, dx}{\int\limits_0^\infty e^{-x} x^\rho \, dx}. \tag{168}$$

Из (168) видно, что производная n-го порядка по ρ от выражения (163) выражается дробью, у которой знаменатель есть

$$\left[\int\limits_0^\infty e^{-x} x^\rho \, dx \right]^{n+1},$$

а числитель — целая функция интегралов $\int\limits_0^\infty \left(\frac{1}{e^x - 1} - \frac{1}{x} \right) e^{-x} x^\rho \, dx$, $\int\limits_0^\infty \left(\frac{1}{e^x - 1} - \frac{1}{x} \right) e^{-x} x^\rho \ln x \, dx, \ldots \int\limits_0^\infty \left(\frac{1}{e^x - 1} - \frac{1}{x} \right) e^{-x} x^\rho \ln^n x \, dx, \int\limits_0^\infty e^{-x} x^\rho dx$ $\int\limits_0^\infty e^{-x} x^\rho \ln x \, dx, \ldots \int\limits_0^\infty e^{-x} x^\rho \ln^n x \, dx$.

Эта дробь при $\rho \to 0$ стремится к конечному пределу, так как знаменатель ее стремится к единице, а интегралы в числителе при $\rho \to 0$ остаются конечными и непрерывными.

Переходим к выражению (164). Имеем по формуле Эйлера (см. § 13, теорему 24):

$$\prod \left(1 - \frac{1}{\mu^{1+\rho}}\right)^{-1} = 1 + \sum \frac{1}{m^{1+\rho}};$$

логарифмируем обе части:

$$-\sum \ln \left(1 - \frac{1}{\mu^{1+\rho}}\right) = \ln \left[1 + \sum \frac{1}{m^{1+\rho}}\right];$$

прибавляем к обеим частям $\ln \rho$:

$$\ln \rho - \sum \ln \left(1 - \frac{1}{\mu^{1+\rho}}\right) = \ln \left[\left(1 + \sum \frac{1}{m^{1+\rho}}\right) \rho\right] =$$
$$= \ln \left[1 + \rho + \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}\right) \rho\right].$$

Левая часть этого равенства и есть выражение (164). Это равенство показывает, что производные по ρ выражения (164) выражаются конечным числом дробей с знаменателями:

$$\left[1 + \rho + \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}\right) \rho\right], \quad (n \text{ — натуральное}),$$

а числители этих дробей — целые функции от ρ, от выражения (163) и от его производных по ρ. Но мы доказали, что выражение (163) и его производные по ρ при $\rho \to 0$ стремятся к конечным пределам, в частности:

$$\lim_{\rho \to 0} \left[1 + \rho + \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}\right) \rho\right] = 1.$$

Отсюда следует, что и выражение (164) и все его производные стремятся к конечным пределам при $\rho \to 0$.

Переходим к выражению (165); его первая производная по ρ:

$$\sum \frac{1}{\mu^{2+2\rho}} \frac{\ln \mu}{1 - \dfrac{1}{\mu^{1+\rho}}};$$

его высшие производные выразятся конечным числом членов вида:

$$\sum \frac{1}{\mu^{2+2\rho}} \frac{\ln^p \mu}{1 - \dfrac{1}{\mu^{1+\rho}}} \frac{1}{\mu^s \left(1 - \dfrac{1}{\mu^{1+\rho}}\right)^r},$$

где p, r, s не < 0. Но все эти члены при $\rho > 0$ и при $\rho = 0$ имеют конечную величину, так как под знаком суммы — выражение, бесконечно-малое относительно $\frac{1}{\mu}$ не ниже 2-го порядка. Следовательно, при $\rho \to 0$ эти выражения стремятся к конечным пределам.

Таким образом, доказано, что производные выражений (163), (164), (165) при $\rho \to 0$ стремятся к конечным пределам.

Следовательно, стремится к конечному пределу и выражение:

$$\frac{d^n\left[\sum \ln\left(1-\frac{1}{\mu^{1+\rho}}\right)+\sum \frac{1}{\mu^{1+\rho}}\right.}{d\rho^n}+\frac{d^n\left|\ln\rho-\sum \ln\left(1-\frac{1}{\mu^{1+\rho}}\right)\right.}{d\rho^n}+$$
$$+\frac{d^{n-1}\left(\sum \frac{1}{m^{1+\rho}}-\frac{1}{\rho}\right)}{d\rho^{n-1}},$$

которое после упрощений принимает вид:

$$\pm\left(\sum \frac{\ln^n \mu}{\mu^{1+\rho}}-\sum \frac{\ln^{n-1} m}{m^{1+\rho}}\right). \tag{169}$$

Но выражение (162) равно разности выражений:

$$\sum_{x=2}^{\infty}[\varphi(x+1)-\varphi(x)]\frac{\ln^n x}{x^{1+\rho}}=\sum \frac{\ln^n \mu}{\mu^{1+\rho}}$$

и

$$\sum_{x=2}^{\infty}\frac{\ln^{n-1}x}{x^{1+\rho}}=\sum \frac{\ln^{n-1} m}{m^{1+\rho}},$$

т. е. выражению (169) со знаком $+$. Таким образом, и выражение (162) при $\rho \to 0$ стремится к конечному пределу, и значит, теорема 1 доказана.

Имеем далее:

$$\frac{1}{\ln x}-\int_x^{x+1}\frac{dx}{\ln x}=\frac{1}{\ln x}-\frac{1}{\ln(x+\theta)}=\frac{\ln\left(1+\frac{\theta}{x}\right)}{\ln x\ln(x+\theta)},$$

где $0<\theta<1$. Это выражение при $x\to\infty$ — бесконечно малая 1-го порядка относительно $\frac{1}{x}$; следовательно, выражение

$$\left(\frac{1}{\ln x}-\int_x^{x+1}\frac{dx}{\ln x}\right)\frac{\ln^n x}{x^{1+\rho}}$$

при $x\to\infty$ есть бесконечно малая порядка $2+\rho$ относительно $\frac{1}{x}$ и сумма

$$\sum_{x=2}^{\infty}\left(\frac{1}{\ln x}-\int_x^{x+1}\frac{dx}{\ln x}\right)\frac{\ln^n x}{x^{1+\rho}}$$

конечна. Сложив ее с выражением (162), получим:

Следствие. Выражение:

$$\sum_{x=2}^{\infty}\left[\varphi(x+1)-\varphi(x)-\int_{x}^{x+1}\frac{dx}{\ln x}\right]\frac{\ln^n x}{x^{1+\rho}} \qquad (170)$$

при ρ, стремящемся к нулю, стремится к конечному пределу.

§ 77. **Теорема II.** От $x=2$ до $x=\infty$ функция $\varphi(x)$, означающая число простых чисел, меньших x, удовлетворяет бесконечное множество раз и неравенству

$$\varphi(x)>\int_{2}^{x}\frac{dx}{\ln x}-\frac{\alpha x}{\ln^n x} \qquad (171)$$

и неравенству

$$\varphi(x)<\int_{2}^{x}\frac{dx}{\ln x}+\frac{\alpha x}{\ln^n x} \qquad (171a)$$

при каком угодно малом α и при каком угодно большом натуральном n.

Доказательство. Мы докажем теорему для неравенства (171а); для неравенства (171) она доказывается аналогично.

Допустим противное, т. е. что неравенству (171а) удовлетворяет конечное число чисел x. Пусть a — целое число такое, что $a>e^n$ и больше наибольшего значения x, удовлетворяющего неравенству (171а). В таком случае при $x>a$ будет:

$$\varphi(x)\geqq\int_{2}^{x}\frac{dx}{\ln x}+\frac{\alpha x}{\ln^n x}; \qquad (172)$$

из $a>e^n$ следует: $\ln x>n$. Следовательно,

$$\varphi(x)-\int_{2}^{x}\frac{dx}{\ln x}\geqq\frac{\alpha x}{\ln^n x}, \quad \frac{n}{\ln x}<1. \qquad (172a)$$

Но в таком случае, как мы докажем, выражение (170) при $\rho\to 0$ беспредельно возрастает, тогда как мы доказали, что оно стремится к конечному пределу.

Выражение (170) можно написать в виде

$$\lim_{s\to\infty}\sum_{x=2}^{s}\left[\varphi(x+1)-\varphi(x)-\int_{x}^{x+1}\frac{dx}{\ln x}\right]\frac{\ln^n x}{x^{1+\rho}}. \qquad (170a)$$

Предполагая, что $s>a$, выражение справа от знака lim можно представить в виде

$$C+\sum_{x=a+1}^{s}\left[\varphi(x+1)-\varphi(x)-\int_{x}^{x+1}\frac{dx}{\ln x}\right]\frac{\ln^n x}{x^{1+\rho}}, \qquad (173)$$

где

$$C=\sum_{x=2}^{a}\left[\varphi(x+1)-\varphi(x)-\int_{x}^{x+1}\frac{dx}{\ln x}\right]\frac{\ln^n x}{x^{1+\rho}};$$

C — имеет конечное значение и при $\rho>0$ и при $\rho=0$.

К выражению (173) мы применим следующую формулу, которую легко проверить:

$$\sum_{x=a+1}^{s}u_x(v_{x+1}-v_x)=u_s v_{s+1}-u_a v_{a+1}-\sum_{x=a+1}^{s}v_x(u_x-u_{x-1}).$$

Положим:

$$v_x=\varphi(x)-\int_{2}^{x}\frac{dx}{\ln x},\qquad u_x=\frac{\ln^n x}{x^{1+\rho}};$$

в таком случае выражение (179) преобразуется в следующее:

$$\left.\begin{aligned}C-\left[\varphi(a+1)-\int_{2}^{a+1}\frac{dx}{\ln x}\right]\frac{\ln^n a}{a^{1+\rho}}+\left[\varphi(s+1)-\int_{2}^{s+1}\frac{dx}{\ln x}\right]\frac{\ln^n s}{s^{1+\rho}}-\\-\sum_{x=a+1}^{s}\left[\varphi(x)-\int_{2}^{x}\frac{dx}{\ln x}\right]\left[\frac{\ln^n x}{x^{1+\rho}}-\frac{\ln^n(x-1)}{(x-1)^{1+\rho}}\right]\end{aligned}\right\}\quad(173а)$$

Имеем:

$$\frac{d}{dx}\left(\frac{\ln^n x}{x^{1+\rho}}\right)=\left[\frac{n}{\ln x}-(1+\rho)\right]\frac{\ln^n x}{x^{2+\rho}}.$$

Применяя теорему о среднем значении Лагранжа, найдем:

$$-\left[\frac{\ln^n x}{x^{1+\rho}}-\frac{\ln^n(x-1)}{(x-1)^{1+\rho}}\right]=\left[1+\rho-\frac{n}{\ln(x-\theta)}\right]\frac{\ln^n(x-\theta)}{(x-\theta)^{2+\rho}},$$

где $0<\theta<1$; θ, конечно, зависит от x. И выражение (173а) примет вид:

$$\left.\begin{aligned}C-\left[\varphi(a+1)-\int_{2}^{a+1}\frac{dx}{\ln x}\right]\frac{\ln^n a}{a^{1+\rho}}+\left[\varphi(s+1)-\int_{2}^{s+1}\frac{dx}{\ln x}\right]\frac{\ln^n s}{s^{1+\rho}}+\\+\sum_{x=a+1}^{s}\left[\varphi(x)-\int_{2}^{x}\frac{dx}{\ln x}\right]\left[1+\rho-\frac{n}{\ln(x-\theta)}\right]\frac{\ln^n(x-\theta)}{(x-\theta)^{2+\rho}}.\end{aligned}\right\}\quad(173б)$$

Обозначив два первых члена этого выражения через F и замечая, что по (172а) третий его член >0, мы заключаем, что все выражение (173б) больше, чем:

$$F+\sum_{x=a+1}^{s}\left[\varphi(x)-\int_{2}^{x}\frac{dx}{\ln x}\right]\left[1+\rho-\frac{n}{\ln(x-\theta)}\right]\frac{\ln^n(x-\theta)}{(x-\theta)^{2+\rho}}.\quad(174)$$

Из тех же неравенств (172а) заключаем, что функция, стоящая под знаком суммы в (174), в пределах суммирования положительна; и, кроме того,

$$1+\rho-\frac{n}{\ln(x-\theta)}>1-\frac{n}{\ln a},$$

так как $\rho>0$, $x\geqq a+1$, $\theta<1$. Далее:

$$\varphi(x)-\int_2^x\frac{dx}{\ln x}>\frac{\alpha(x-\theta)}{\ln^n(x-\theta)}, \tag{175}$$

ибо по первому неравенству (172а) левая часть (175) не меньше $\frac{\alpha x}{\ln^n x}$. Но

$$\frac{\alpha x}{\ln^n x}>\frac{\alpha(x-\theta)}{\ln^n(x-\theta)},$$

что́ следует из того, что функция $\frac{\alpha x}{\ln^n x}$ возрастает вместе с x, так как ее производная

$$\frac{\alpha}{\ln^n x}\left(1-\frac{n}{\ln x}\right)>0$$

(по второму неравенству (172а)). Итак выражение (174) больше, чем:

$$F+\sum_{x=a+1}^{s}\frac{\alpha(x-\theta)}{\ln^n(x-\theta)}\left(1-\frac{n}{\ln a}\right)\frac{\ln^n(x-\theta)}{(x-\theta)^{2+\rho}}.$$

Упростив это выражение, получим:

$$F+a\left(1-\frac{n}{\ln a}\right)\sum_{x=a+1}^{s}\frac{1}{(x-\theta)^{1+\rho}},$$

а это — больше, чем

$$F+\alpha\left(1-\frac{n}{\ln a}\right)\sum_{x=a+1}^{s}\frac{1}{x^{1+\rho}};$$

для $s=\infty$ это будет:

$$F+\alpha\left(1-\frac{n}{\ln a}\right)\sum_{x=a+1}^{\infty}\frac{1}{x^{1+\rho}}. \tag{176}$$

Но аналогично формуле (166) легко вывести, что

$$\int_0^\infty\frac{e^{-ax}}{e^x-1}x^\rho dx=\sum_{m=a+1}^{\infty}\frac{1}{m^{1+\rho}}\cdot\int_0^\infty e^{-x}x^\rho dx.$$

Следовательно, выражение (176) представляется в виде:

$$F+\alpha\left(1-\frac{n}{\ln a}\right)\frac{\int\limits_0^\infty \frac{e^{-\alpha x}}{e^x-1}x^\rho dx}{\int\limits_0^\infty e^{-x}x^\rho dx}.$$

Но при $\rho\to 0$ это выражение беспредельно возрастает, так как интеграл в знаменателе стремится к 1, а интеграл в числителе беспредельно возрастает.

Отсюда следует, что и выражение (170) при $\rho\to 0$ беспредельно возрастает, а это противоречит теореме I. Таким образом, теорема II доказана.

§ 78. Теорема III. Выражение $\frac{x}{\varphi(x)}-\ln x$ при $x\to\infty$ не может иметь пределом количество, отличное от -1.

Доказательство. Пусть $L=\lim\limits_{x\to\infty}\left[\frac{x}{\varphi(x)}-\ln x\right]$; тогда при достаточно большом $x>N$ будем иметь:

$$L-\varepsilon<\frac{x}{\varphi(x)}-\ln x<L+\varepsilon \qquad (177)$$

при как угодно малом $\varepsilon>0$.

Но по теореме II неравенства (171) и (171а) удовлетворяются при бесчисленном множестве значений x, а следовательно, и при некоторых (бесчисленном множестве) значениях $x>N$. Для таких значений (177) дает:

$$\frac{x}{\int\limits_2^x \frac{dx}{\ln x}-\frac{\alpha x}{\ln^n x}}-\ln x>L-\varepsilon;$$

$$\frac{x}{\int\limits_2^x \frac{dx}{\ln x}+\frac{\alpha x}{\ln^n x}}-\ln x<L+\varepsilon.$$

Отсюда получим:

$$L+1<\frac{x-(\ln x-1)\left(\int\limits_2^x \frac{dx}{\ln x}-\frac{\alpha x}{\ln^n x}\right)}{\int\limits_2^x \frac{dx}{\ln x}-\frac{\alpha x}{\ln^n x}}+\varepsilon;$$

$$L+1>\frac{x-(\ln x-1)\left(\int\limits_2^x \frac{dx}{\ln x}+\frac{\alpha x}{\ln^n x}\right)}{\int\limits_2^x \frac{dx}{\ln x}+\frac{\alpha x}{\ln^n x}}-\varepsilon.$$

Из этих неравенств видно, что $|L+1|$ не превссходит абсолютной величины одного из выражений:

$$\frac{x-(\ln x-1)\left(\int\limits_2^x \frac{dx}{\ln x} \mp \frac{\alpha x}{\ln^n x}\right)}{\int\limits_2^x \frac{dx}{\ln x} \mp \frac{\alpha x}{\ln^n x}} \pm \varepsilon. \tag{178}$$

Но ε может быть взято каким угодно малым; что́ же касается дроби в выражении (178), то при $x \to \infty$ она стремится к нулю. Мы найдем это, продифференцировав отдельно числитель и знаменатель и найдя (по правилу Лопиталя) предел отношения полученных производных. Но производная знаменателя:

$$\frac{1}{\ln x} \mp \frac{\alpha}{\ln^n x} \pm \frac{n\alpha}{x \ln^{n+1} x},$$

а производная числителя:

$$1-\frac{1}{x}\left(\int\limits_2^x \frac{dx}{\ln x} \mp \frac{\alpha x}{\ln^n x}\right)-(\ln x-1)\left(\frac{1}{\ln x} \mp \frac{\alpha}{\ln^n x} \pm \frac{n\alpha}{x \ln^{n+1} x}\right)=$$

$$=1-\frac{1}{x}\int\limits_2^x \frac{dx}{\ln x} \pm \frac{\alpha}{\ln^n x}-1 \pm \frac{\alpha}{\ln^{n-1} x} \mp \frac{n\alpha}{x \ln^n x}+\frac{1}{\ln x} \mp \frac{\alpha}{\ln^n x} \pm \frac{n\alpha}{x \ln^{n+1} x}=$$

$$=\frac{1}{\ln x}-\frac{1}{x}\int\limits_2^x \frac{dx}{\ln x} \pm \frac{\alpha}{\ln^{n-1} x} \mp \frac{n\alpha}{x \ln^n x} \pm \frac{n\alpha}{x \ln^{n+1} x}.$$

Берем отношение производной числителя к производной знаменателя:

$$\frac{1-\frac{\ln x}{x}\int\limits_2^x \frac{dx}{\ln x} \pm \frac{\alpha}{\ln^{n-2} x} \mp \frac{n\alpha}{x \ln^{n-1} x} \pm \frac{n\alpha}{x \ln^n x}}{1 \mp \frac{\alpha}{\ln^{n-1} x} \pm \frac{n\alpha}{x \ln^n x}}. \tag{179}$$

При $x \to \infty$ знаменатель полученной дроби стремится к 1; в числителе же 3-й, 4-й и 5-й члены стремятся к нулю. Что касается выражения:

$$\frac{\ln x}{x}\int\limits_2^x \frac{dx}{\ln x}=\int\limits_2^x \frac{dx}{\ln x} : \frac{x}{\ln x},$$

то для нахождения его предела при $x \to \infty$ применим снова правило Лопиталя:

$$\lim_{x\to\infty}\left(\frac{\ln x}{x}\int\limits_2^x \frac{dx}{\ln x}\right)=\lim_{x\to\infty}\left[\frac{1}{\ln x} : \frac{\ln x-1}{\ln^2 x}\right]=\lim_{x\to\infty}\left(\frac{\ln x}{\ln x-1}\right)=1.$$

Итак, предел дроби (179) при $x \to \infty$ равен нулю.

Таким образом, получаем, что $|L+1|$ может быть сделано каким угодно малым при достаточно большом x; а так как $L+1$ не зависит от x, то заключаем, что $L+1=0$, $L=-1$, и теорема III доказана.

Доказанная теорема опровергает формулу Лежандра (см. (161)), по которой при больших значениях x можно принять:

$$\varphi(x) = \frac{x}{\ln x - 1{,}08366},$$

откуда:

$$\frac{x}{\varphi(x)} - \ln x = -1{,}08366.$$

Таков и предел этого выражения при $x \to \infty$, а по теореме III этот предел, если он существует, должен быть равен -1.

Но существующие таблицы простых чисел слишком малы, чтобы усмотреть из них превосходство формулы Чебышева $\int\limits_2^x \frac{dx}{\ln x}$ перед формулой Лежандра (161). Оба эти выражения в пределах существующих таблиц мало разнятся друг от друга. Но разность:

$$\frac{x}{\ln x - 1{,}08366} - \int\limits_2^x \frac{dx}{\ln x}$$

имеет минимум при $x = e^{\frac{(1{,}08366)^2}{0{,}08366}} \approx 1247689$; при дальнейшем возрастании эта разность беспредельно возрастает.

В конце рассматриваемой работы Чебышев исправляет две формулы, которые при применении предположения Лежандра имели неправильный вид. Именно:

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots + \frac{1}{x} = C + \ln\ln x$$

$$(\text{а не } C + \ln(\ln x - 0{,}08366));$$

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\ldots\left(1-\frac{1}{x}\right) = \frac{C_0}{\ln x}$$

$$\left(\text{а не } \frac{C_0}{\ln x - 0{,}08366}\right).$$

Здесь C и C_0 — определенные постоянные, не зависящие от x.

§ 79. Упомянем теперь о других работах Чебышева по теории чисел.

В работе «О простых числах» (1850 г.) Чебышев вводит и исследует арифметическую функцию $\theta(x) = \sum\limits_{p \leq x} \ln p$ (сумма берется по всем простым числам $p \leq x$). При помощи этой функции он доказывает постулат Бертрана (мы о нем упоминали в § 14): «при $a > 3$ между a и $2a-2$ находится по крайней мере одно простое число».

Чебышев доказывает его для чисел $a > 160$; при $a \leqq 160$ этот постулат проверяется непосредственно.

В этой же работе доказывается и следующая теорема: «Если при достаточно большом x функция $F(x)$ положительна, то необходимое и достаточное условие сходимости ряда $\sum_p F(p)$ (где p пробегает все простые числа) есть сходимость ряда $\sum_{m=2}^{\infty} \frac{F(m)}{\ln m}$ (m пробегает все натуральные числа, начиная с 2)».

Таким образом, например, получается, что ряд $\sum_p \frac{1}{p}$ расходящийся, тогда как ряд $\sum_p \frac{1}{p \ln p}$ сходящийся.

Е. Ландау заметил, что из результатов Чебышева получается более общая теорема, чем постулат Бертрана, а именно: «При $\varepsilon > \frac{1}{5}$ между x и $(1+\varepsilon)x$ находится, начиная с определенного x, по крайней мере одно простое число; начиная с определенного (бо́льшего) x, — по крайней мере два простых числа и т. д.; начиная с определенного x, — по крайней мере q простых чисел при произвольном натуральном q. Отсюда следует: если p_n n-е простое число, то

$$\limsup_{n \to \infty} \frac{p_{n+1}}{p_n} \leqq \frac{6}{5}.$$

В 1896 г. Адамар и независимо от него Валле-Пуссен дополнили результаты Чебышева, доказав, что существуют пределы: $\lim_{x \to \infty} \frac{\varphi(x) \ln x}{x}$ и $\lim_{x \to \infty} \frac{\theta(x)}{x}$. Из исследований Чебышева следует, что если эти пределы существуют, то они оба $= 1$.

А из существования этих пределов следует, что:

$$\lim_{n \to \infty} \frac{p_{n+1}}{p_n} = 1,$$

где p_n, как и раньше, n-е простое число.

В работе «О квадратичных формах» (1851 г.) Чебышев рассматривает формы вида $x^2 - Dy^2$ и ставит задачу: найти критерий простоты числа N в зависимости от его представления такой формой. Он доказывает теоремы:

1. Если уравнение $x^2 - Dy^2 = \pm N$ имеет две различных системы целых решений x, y в пределах для x от 0 до $\sqrt{\frac{(\alpha \pm 1) N}{2}}$ и для y от 0 до $\sqrt{\frac{(\alpha \mp 1) N}{2D}}$, то N — составное.

Здесь α, β — наименьшее положительное решение уравнения $\alpha^2 - D\beta^2 = 1$.

2. Если все делители формы $x^2 - Dy^2$ имеют форму $\lambda x^2 - \mu y^2$, а N, взаимно-простое с D, имеет вид одного из делителей квадратичной формы $\pm(x^2 - Dy^2)$, то N простое число, если в пределах $x = 0$, $x = \sqrt{\frac{(\alpha + 1)N}{2}}$ и $y = 0$, $y = \sqrt{\frac{(\alpha \mp 1)N}{2D}}$ имеется только одно решение уравнения $\pm(x^2 - Dy^2) = N$ при x, y взаимно-простых. Во всех иных случаях число N — составное (α — то же, что и в первой теореме).

Чебышев приводит таблицу форм: $\pm(x^2 - Dy^2)$ при $D = 2$, 3, ... 33 вместе с пределами $\sqrt{\frac{(\alpha \pm 1)N}{2}}$, $\sqrt{\frac{(\alpha \mp 1)N}{2D}}$ и с линейными делителями этих форм. Под конец он исследует число 8520191 при помощи формы $3y^2 - x^2$ и выявляет, что это число простое. Это число Чебышев взял из одного примера Лежандра (Théorie des nombres, t. II, part IV, § 17). Лежандр, следуя правилу математика Табит-ибн-Курра (IX в., родом из Месопотамии) образования «дружественных чисел» (см. § 17), приводит числа:

$$A = 2^8 \cdot 8520191, \quad B = 2^8 \cdot 257 \cdot 33023.$$

Эти числа дружественные, если числа 257, 33023, 8520191 — простые. Лежандр знал, что 257 и 33023 — простые числа, но не знал, простое ли число 8520191; простоту этого числа и доказал Чебышев.

§ 80. От изучения свойств целых чисел теория чисел, естественно, обратилась к изучению иных родов чисел. Дроби не представляют собой ничего сложного и давно уже были изучены как частные целых чисел. Гораздо более сложными являются иррациональные числа. Уже давно было обращено внимание на два рода иррациональных чисел: числа алгебраические, являющиеся корнями алгебраических уравнений с целыми коэффициентами, и числа трансцендентные, не являющиеся корнями никакого алгебраического уравнения с целыми коэффициентами. Еще Эйлер в своей книге «Введение в анализ» (1744 г.) высказал утверждение, что при рациональном основании a логарифм любого рационального числа b, не являющегося рациональной степенью числа a, не может быть даже числом «иррациональным» (т. е. алгебраическим) и должен относиться к количествам трансцендентным. Это утверждение доказано только в наше время.

Только в 1844 г. Лиувиль доказал существование трансцендентных чисел, дав необходимый признак для алгебраического числа, а следовательно, и достаточный признак трансцендентности числа.

Алгебраические числа, как более простые, были изучены уже в XIX столетии. При этом, говоря об алгебраических числах, имели в виду корни алгебраических уравнений с целыми коэффициентами,— независимо от того, вещественны ли эти корни или комплексны. Обычные рациональные — целые или дробные числа — тоже являются частным случаем алгебраических: это — корни алге-

браических уравнений 1-й степени с целыми коэффициентами. Имеет место следующая теорема:

Сумма, разность, произведение и частное алгебраических чисел — тоже алгебраические числа. Т. е. все алгебраические числа составляют *поле* или *область рациональности*.

Среди алгебраических чисел особенно важное значение имеют те, которые являются корнями алгебраических уравнений с целыми коэффициентами и *с высшим коэффициентом, равным единице*. Корни таких уравнений называются целыми алгебраическими числами, причем доказывается, что сумма, разность и произведение целых алгебраических чисел — тоже целые алгебраические числа, т. е. совокупность всех целых алгебраических чисел есть *область целости*.

Частное двух целых алгебраических чисел — не всегда целое число. Поэтому в области целых алгебраических чисел возникает вопрос о делимости: целое число α делится на целое число β, если частное $\frac{\alpha}{\beta}$ тоже целое число. Но здесь следует обратить внимание на два обстоятельства:

Во-первых, в области всех целых алгебраических чисел нет никакого аналога простым числам, т. е. нет «неразложимых» чисел, так как если α — целое число, то $\sqrt{\alpha}$ тоже целое число и $\alpha = \sqrt{\alpha} \cdot \sqrt{\alpha}$. Поэтому нецелесообразно рассматривать целые алгебраические числа во всей своей совокупности. Рассматривают обычно целые алгебраические числа, являющиеся рациональными функциями (с рациональными коэффициентами) от корня α некоторого неприводимого уравнения $F(x) = 0$ с целыми коэффициентами, или, как говорят, целые числа в *алгебраическом поле* $P(\alpha)$, полученном от *присоединения* числа α к области P всех обычных рациональных чисел.

Во-вторых, существуют целые алгебраические числа, которые являются делителями всякого целого алгебраического числа. Это именно делители единицы, т. е. такие целые числа ε, что и $\frac{1}{\varepsilon}$ — целое число; такие числа называются «алгебраическими единицами». В области целых рациональных чисел таких единиц только две: 1 и —1. В алгебраическом же поле $P(\alpha)$ алгебраических единиц вообще бесчисленное множество. В вопросах делимости единичный множитель роли не играет, ибо если целое число α делится на целое число β, а ε_1 и ε_2 — любые алгебраические единицы, то $\alpha\varepsilon_1$ делится на $\beta\varepsilon_2$. Такие числа, как α и $\alpha\varepsilon_1$, т. е. отличающиеся друг от друга единичным множителем, называются *ассоциированными*; в вопросах делимости они играют одну и ту же роль и могут быть заменены одно другим.

В алгебраическом поле $P(\alpha)$ существуют «неразложимые» целые числа, т. е. такие, которые делятся только на «единицы» и на ассоциированные с собой числа. Легко доказать, что всякое целое число μ из $P(\alpha)$ представляется как произведение таких «нераз-

ложимых» чисел. Но такое представление вообще не однозначно, поэтому аналогии этих неразложимых чисел с обычными простыми числами нет. Например, в области $P(\sqrt{-11})$ имеем два разложения числа 15:

$$15 = 3 \cdot 5 = (2 + \sqrt{-11})(2 - \sqrt{-11});$$

числа 3, 5, $2 + \sqrt{-11}$; $2 - \sqrt{-11}$ неразложимы и не ассоциированы друг с другом.

Еще Гаусс в 1832 г. в работе «Теория биквадратичных вычетов» *) рассмотрел целые числа в поле $P(i)$, т. е. числа вида $a + bi$ («комплексные числа Гаусса»), где a и b — обычные целые числа. Эйзенштейн **) рассмотрел целые числа в поле $P(\omega)$, где $\omega = \frac{-1 + i\sqrt{3}}{2}$ — так называемый первообразный кубический корень из единицы, т. е. числа вида $a + b\omega$, где a, b — обычные целые числа.

Обе эти теории — и целых чисел Гаусса, и целых чисел Эйзенштейна — вполне аналогичны теории делимости обычных целых чисел. В каждой из них имеется теорема о делении с остатком, верен алгорифм Эвклида, есть понятие об общем наибольшем делителе, а на этом основана однозначность разложения числа на неразложимые множители, которая, таким образом, имеет место и в поле $P(i)$ и в поле $P(\omega)$. Заметим, что в поле $P(i)$ имеется всего четыре алгебраических единицы: ± 1 и $\pm i$, а в поле $P(\omega)$ — шесть алгебраических единиц: ± 1, $\pm \omega$, $\pm \omega^2$.

Куммер в 1847 г. ***) в связи со своими исследованиями великой теоремы Ферма рассмотрел целые числа в поле $P(\varepsilon)$, где $\varepsilon = e^{\frac{2\pi i}{n}}$ — первообразный корень n-й степени из единицы. Оказалось, что в поле $P(\varepsilon)$ при произвольном натуральном n неверна теорема об однозначном разложении на неразложимые множители. Но ее справедливость восстановится, если ввести подходящим образом некоторые алгебраические числа, не принадлежащие к полю $P(\varepsilon)$, которые Куммер назвал «идеальными» числами.

Но общую теорию целых чисел в любом алгебраическом поле $P(\alpha)$ разработал: **Егор Иванович Золотарев** (1847—1878) в своей докторской диссертации «Теория целых комплексных чисел с приложением к интегральному исчислению» (СПб., 1874).

Е. И. Золотарев родился и учился в Петербурге; в 1867 г. кончил Петербургский университет. С 1868 г. преподавал в Петербургском университете в качестве приват-доцента, в 1876 г. был избран профессором Петербургского университета и в том же году — адъюнктом Академии наук. Летом 1878 г. Е. И. Золотарев трагически погиб, попав под паровоз.

*) Theoria residuorum biquadraticorum. (Ges. Werke, том II).

**) В журн. Crelle, т. 27 и 28.

***) Theorie der idealen Primfaktoren der komplexen Zahlen... Журн. Crelle, т. 35.

«Целыми комплексными» числами Золотарев называет целые алгебраические числа. Докторская диссертация Золотарева разделяется на четыре главы:

Гл. I. «О функциональных сравнениях».

Гл. II. «О комплексных единицах».

Гл. III. «Идеальные множители комплексных чисел».

Гл. IV. «Приложение теории комплексных чисел к одному вопросу интегрального исчисления».

Последняя глава к теории чисел не относится. В гл. I излагается общая теория разложения целочисленных многочленов на простые (т. е. неприводимые) множители по модулю p (p — простое число). В гл. II Золотарев дает свое доказательство теоремы Дирикле об алгебраических единицах. Самая важная гл. III, представляющая собственные исследования Золотарева.

Если $P(\alpha)$ — данное алгебраическое поле, α — корень неприводимого уравнения $F(x)=0$ с целыми коэффициентами и высшим коэффициентом $=1$, а p — обычное простое число, то может случиться, что $F(x)$ — простой (неприводимый) многочлен по модулю p. В этом случае, как доказывает Золотарев, произведение целых чисел из $P(\alpha)$ тогда и только тогда делится на p, когда один из сомножителей делится на p и число p простое и в области $P(\alpha)$. В противном же случае будет:

$$F(x) = V^m V_1^{m_1} \ldots V_s^{m_s} + pF_1(x),$$

где V, V_1, ... V_s — многочлены, простые по модулю p.

Если хоть один из показателей m, m_1, ... m_s больше 1, то, как показывает Золотарев, p — делитель дискриминанта D многочлена F. Если среди простых делителей p дискриминанта D имеется такой, для которого $F_1(x)$ делится по модулю p хоть на один множитель V_l (при $m_l > 1$), то такой многочлен $F(x)$ Золотарев назвал «особенным». Случай «особенного» многочлена он рассмотрел позднее; этот случай изложен в его работах «О комплексных числах» («Sur les nombres complexes», 1878) и «О теории комплексных чисел» («Sur la theorie des nombres complexes», 1885,— посмертная работа).

Если обычное простое число p — не простое в поле $P(\alpha)$, то Золотарев представляет p состоящим из идеальных простых множителей:

$$p = \pi^m \pi_1^{m_1} \ldots \pi_s^{m_s}.$$

Золотарев доказывает, что каждое целое число из поля $P(\alpha)$ содержит идеальные множители только тех простых чисел, которые являются делителями его нормы. Так всякое целое число из $P(\alpha)$, однозначно раскладывается на простые идеальные множители.

Этой своей фундаментальной работой Золотарев положил основу общей теории алгебраических чисел.

Заметим, что только четыре года спустя после Золотарева, в 1878 г. Дедекинд построил на других основах теорию алгебраиче-

ских чисел,— так называемую «теорию идеалов» (в приложении к 3-му изданию лекций Дирикле по теории чисел). Профессор Петербургского университета И. И. Иванов (1862—1939) в своей магистерской диссертации «К теории целых комплексных чисел» (1893 г.) установил эквивалентность теорий алгебраических чисел Золотарева и Дедекинда.

Упомянем еще о совместных работах Золотарева и Коркина *) о минимумах положительных квадратичных форм.

§ 81. Георгий Федосеевич Вороной (1868—1908) родился в Полтавской губернии, учился в Петербургском университете. В своих диссертациях — магистерской и докторской — он разработал теорию кубических иррациональностей, т. е. алгебраических чисел, являющихся корнями кубических уравнений с целыми коэффициентами.

Магистерская диссертация Г. Ф. Вороного «О целых алгебраических числах, зависящих от корня уравнения 3-й степени» (СПб., 1894), состоит из трех глав.

Гл. I. «О комплексных числах по модулю p. Приложение их к решению сравнения $X^3-rX-s\equiv 0 \pmod p$ при p простом. Некоторые вспомогательные величины».

Здесь дается способ решения сравнений 3-й степени $X^3-rX-s\equiv 0 \pmod p$ по простому модулю p. Вводятся «комплексные числа по модулю p», т. е. числа вида $X+X'i$, где X, X' — целые, а i не существующее число, удовлетворяющее сравнению: $i^2\equiv N \pmod p$, где N квадратичный невычет числа p. Доказывается теорема: «Если дискриминант данного сравнения 3-й степени $-\Delta = 4r^3-27s^2$ — квадратичный невычет числа p, то сравнение имеет всегда и только одно решение по модулю p; если же этот дискриминант — квадратичный вычет числа p, то сравнение или имеет три решения, или не имеет ни одного решения».

Гл. II. «Разыскание трех основных алгебраических чисел, из которых сложением и вычитанием получаются все целые алгебраические числа, зависящие от корня уравнения $\rho^3=r\rho+s$».

Здесь доказывается основная теорема: «Все целые алгебраические числа, зависящие от корня неприводимого уравнения $\rho^3=r\rho+s$, заключаются в форме:

$$X+X'\frac{-\xi+\rho}{\delta}+X''\frac{\xi^2-r+\xi\rho+\rho^2}{\delta^2\sigma},$$

где X, X', X'' — любые целые рациональные числа; ξ — единственное решение по модулю $\delta\sigma$ сравнений

$$\xi^3-r\xi-s\equiv 0 \pmod{\delta^3\sigma^2},\quad 3\xi^2-r\equiv 0 \pmod{\delta^2\sigma}».$$

(Целые числа δ и σ, постоянные для данного поля, находятся определенным образом).

---

*) Александр Николаевич Коркин (1837—1908) был профессором Петербургского университета. О его способе решения сравнений мы уже говорили в § 53.

Гл. III. «Идеальные множители целых алгебраических чисел, зависящих от корня уравнения $\rho^3 = r\rho + s$».

Здесь даются разложения на простые идеальные множители всех целых чисел кубической области.

Докторская диссертация Г. Ф. Вороного «Об одном обобщении алгорифма непрерывных дробей» (Варшава, 1896) состоит из предисловия и трех отделов.

Отд. I. «Последовательные относительные минимумы системы ковариантных форм $\omega = X\lambda + X'\mu$ и $\omega' = X\lambda' + X'\mu'$ при целых рациональных значениях переменных».

Здесь рассматриваются обыкновенные цепные дроби, но с новой точки зрения, которая кладется в основу их обобщения.

Отд. II. «Последовательные относительные минимумы системы ковариантных форм $\omega = X\lambda + X'\mu + X''\nu$ и $\omega' = X(l' + l''i) + X'(m' + m''i) + X''(n' + n''i)$ при целых рациональных значениях переменных».

Здесь выводятся необходимые и достаточные условия эквивалентности систем ковариантных форм. Полученные результаты применяются к системам форм, зависящих от корней уравнения 3-й степени с отрицательным дискриминантом. Доказывается, что при преобразовании таких систем введенным Г. Ф. Вороным алгорифмом получается ряд периодически повторяющихся приведенных форм. Приводится способ получения основной алгебраической единицы и способ определения числа классов неэквивалентных идеалов в данной кубической области.

Отд. III. «Последовательные относительные минимумы системы ковариантных форм $\omega = X\lambda + X'\mu + X''\nu$, $\omega' = X\lambda' + X'\mu' + X''\nu'$ и $\omega'' = X\lambda'' + X'\mu'' + X''\nu''$ при целых рациональных значениях переменных».

Здесь дается алгорифм преобразования системы ковариантных форм, коэффициенты которых зависят от корней уравнения 3-й степени с положительным дискриминантом. Доказывается, что получается ряд периодически повторяющихся приведенных систем. Выводится способ для получения основной системы алгебраических единиц и для определения числа классов неэквивалентных идеалов данной области.

В своих исследованиях по теории чисел Г. Ф. Вороной широко применял геометрические средства. Этот геометрический метод применялся им и в других его работах, а именно: «О некоторых свойствах совершенных положительных форм» (1907) и «Исследования о первообразных параллелоэдрах» (1908); там излагается теория квадратичных форм с n переменными. Таким образом Г. Ф. Вороной разделяет с Г. Минковским приоритет по созданию так называемой геометрической теории чисел.

Большое значение имеет работа Г. Ф. Вороного «Об одной задаче из теории асимптотических функций» (1908). Здесь рассматривается приближенное вычисление суммы: $\sum_{k=1}^{m} \tau(k)$, где $\tau(k)$ —

число всех делителей числа k (см. § 16). Геометрически это сводится к определению количества точек с целыми положительными координатами в части плоскости, ограниченной осями координат и верхней частью гиперболы $xy = n$. Дирикле дал следующую формулу:

$$\sum_{k=1}^{m} \tau(k) = m(\ln m + 2C - 1) + O(\sqrt{m})\ ^{*)},$$

где $C = 0{,}57721\ldots$ — так называемая Эйлерова постоянная.

С помощью довольно сложных вычислений Вороной вывел более точную формулу:

$$\sum_{k=1}^{m} \tau(k) = m(\ln m + 2C - 1) + O(\sqrt[3]{m}\ln m).$$

К работам Вороного тесно примыкают работы советских математиков: первые работы И. М. Виноградова, некоторые работы Делоне, Житомирского, Венкова.

Как большого специалиста по теории чисел дореволюционного времени следует назвать еще академика **Андрея Андреевича Маркова** (1856—1922); он имеет важные работы во многих областях математики: и в теории алгебраических непрерывных дробей, и в теории конечных разностей, и в теории функций, наименее уклоняющихся от нуля, и в особенности в теории вероятностей. В теории чисел очень важные работы Маркова — о верхнем пределе минимумов неопределенных квадратичных форм.

§ 82. В советское время в нашей стране теория чисел развивалась еще быстрее во всех своих отраслях. Выдающимся специалистом по теории чисел является **Иван Матвеевич Виноградов** — один из крупнейших современных математиков. И. М. Виноградов родился в 1891 г., окончил физико-математический факультет Петербургского университета; в 1915 г. написал свою первую работу о сумме значений символа Лежандра. В 1918—1920 гг. он жил в Перми, состоя сначала доцентом, а затем профессором Пермского университета. В конце 1920 г. И. М. Виноградов вернулся в Петроград; с 1925 г. он был профессором Ленинградского университета; в январе 1929 г. избран действительным членом Академии наук. Вместе с Академией наук И. М. Виноградов переехал в Москву, где работает и в настоящее время. В 1941 г. за книгу «Новый метод в аналитической теории чисел» ему была присуждена Сталинская премия 1-й степени, а в 1945 г. присвоено звание Героя Социалистического Труда.

---

*) Символ $O(g(x))$ означает такую функцию $f(x)$, что при $x \to \infty$ $\frac{|f(x)|}{g(x)}$ остается ограниченным, т. е. существует такое постоянное число $M > 0$, что $\frac{|f(x)|}{g(x)} < M$. Здесь x — вещественная переменная, $f(x)$ — вещественная или комплексная функция, $g(x)$ — вещественная функция > 0.

И. М. Виноградов работает главным образом в аналитической теории чисел; он ввел в эту область свои, новые методы, оказавшиеся очень плодотворными.

Первые работы Виноградова посвящены задачам о вычислении погрешности приближенных формул, содержащих различные числовые функции. Такова задача Дирикле о числе целых точек в области, ограниченной осями координат и гиперболой $xy = n$, и задача о числе целых точек в круге $x^2 + y^2 \leq n$. Эти задачи решал Вороной. Виноградов дал более простой метод, приложимый к широкому классу контуров. Первый общий метод решения задач такого типа приведен в работе Виноградова «Новый способ для получения асимптотических выражений арифметических функций» («Известия АН СССР», 1917).

Группа работ Виноградова относится к распределению вычетов и невычетов данной степени, первообразных корней и т. д. в арифметических прогрессиях или в интервалах заданной длины. При помощи оценок тригонометрических сумм Виноградов выводит ряд относящихся сюда теорем. Например:

1. Наименьший положительный квадратичный невычет для простого модуля p меньше, чем

$$p^{\frac{1}{2\sqrt{e}}}(\ln p)^2.$$

2. Наименьший положительный первообразный корень простого числа меньше, чем

$$2^{2k}\sqrt{p}\ln p,$$

где k — число различных простых делителей числа $p-1$.

Весьма важные результаты Виноградов получил в так называемой проблеме Уоринга (Waring).

В 1770 г. Уоринг высказал такое утверждение: «Для всякого целого показателя $n \geq 2$ существует такое $r = r(n)$, что всякое целое $N > 0$ может быть представлено в форме

$$N = x_1^n + x_2^n + \ldots + x_r^n \tag{180}$$

с целыми $x_i \geq 0$».

Первое общее доказательство этой теоремы было дано только в 1909 году Гильбертом (Hilbert). Но его метод дает слишком большие значения для r. С 1920 по 1926 г. Харди и Литльвуд опубликовали шесть мемуаров под заглавием «Some Problems of Partitio Numerorum» *), где применяют новый общий метод для решения аддитивных проблем теории чисел; мемуары I, II, III, IV посвящены проблеме Уоринга.

Обозначим через $G(n)$ наименьшее значение r при данном n, т. е. такое число, что при всяком $N > N_0$ (т. е. для достаточно больших N) при $r = G(n)$ представление (180) имеет место, тогда как при $r < G(n)$ представление (180) не имеет места для бесчис-

*) «Некоторые проблемы разложения чисел».

ленного множества чисел N. Легко доказывается, что $G(n) > n$. Харди и Литльвуд нашли, что

$$G(n) \leqq (n-2) \cdot 2^{n-1} + 5.$$

И. М. Виноградов начал заниматься проблемой Уоринга с 1924 г. В 1934 г. он открыл новый метод, который позволил резко снизить оценку для $G(n)$. Систематическое изложение этого метода И. М. Виноградов дал в книге «Новый метод в аналитической теории чисел» (1937 г.). Формулы, выведенные Виноградовым, следующие:

$$G(n) < 6n(\ln n + 1) \text{ при } n \geqq 9, \qquad (181)$$

$$G(n) \leqq 2\left[\frac{n(n-2)\ln 2 - 0{,}5}{1+\frac{\nu}{2}}\right] + 2n + 5. \qquad (182)$$

Вторая формула верна и при $n < 9$; $\nu = \frac{1}{n}$.

Формула (181) дает

$$G(n) = O(n \ln n).$$

Из формулы (182) получаем:

$$G(3) \leqq 13,\ G(4) \leqq 21,\ G(5) \leqq 31,$$
$$G(6) \leqq 45,\ G(7) \leqq 63,\ G(8) \leqq 81.$$

При $n \leqq 17$ формула (182) точнее, чем (181); при $n > 17$ наоборот.

Для небольших значений n функция $G(n)$ исследовалась особо. Так, в 1927 г. Э. Ландау доказал, что $G(3) \leqq 8$; в 1936 г. Эстерман, Давенпорт и Хейльброн показали, что $G(4) \leqq 17$. В гл. VI, § 74 мы видели, что $G(2) = 4$; это точное значение для $G(2)$, ибо числа вида $8k + 7$ не представляются в виде сумм трех квадратов.

Наконец, как уже упоминалось в конце § 14, И. М. Виноградов в 1937 г. решил и знаменитую проблему Гольдбаха, доказав теорему о том, что всякое нечетное число N, бо́льшее некоторого предела N_0, может быть представлено в виде суммы трех простых чисел. Отсюда непосредственно следует, что всякое четное число N_1 бо́льшее некоторого предела N_1, может быть представлено в виде суммы четырех простых чисел.

Эта теорема в течение почти двухсот лет не поддавалась усилиям весьма больших специалистов; в 1912 году Э. Ландау высказал мнение, что проблема Гольдбаха недоступна средствам современной математики.

В 1930 году советский математик **Лев Генрихович Шнирельман** (1905—1938) доказал, что всякое целое число > 1 есть сумма ограниченного числа простых чисел; однако граница для этого числа была очень велика. В последующем эта граница была уменьшена до 67; но результат Виноградова снизил ее до 4.

Идея доказательства Виноградова следующая: известно, что интеграл

$$\int_0^1 e^{2\pi i\alpha h} d\alpha, \tag{183}$$

где h — целое число, равен нулю при $h \neq 0$ и равен 1 при $h = 0$.

Пусть дано любое нечетное число $N > 0$ и пусть p_1, p_2, p_3 три простых числа, меньших чем N. Возьмем $h = p_1 + p_2 + p_3 - N$ и подставим в (183), если полученный таким образом интеграл окажется отличным от нуля, то это будет означать, что $N = p_1 + p_2 + p_3$.

Возьмем теперь сумму:

$$I_N = \sum_{p_1 \leqq N} \sum_{p_2 \leqq N} \sum_{p_3 \leqq N} \int_0^1 e^{2\pi i\alpha(p_1+p_2+p_3-N)} d\alpha = \int_0^1 \Big(\sum_{p \leqq N} e^{2\pi i\alpha p} \Big)^3 e^{-2\pi i\alpha N} d\alpha,$$

где p пробегает все простые числа $\leq N$. Если мы докажем, что этот интеграл I_N положителен (не равен нулю), то тем самым будет доказано, что всякое целое число $N > 0$ представляется как сумма трех простых чисел. Если, кроме того, мы найдем приближенное значение интеграла I_N, то этим будет найдено приближенно и число различных представлений N в виде суммы трех простых чисел. Виноградову удалось доказать, что $I_N > 0$, и найти его приближенное значение для всех достаточно больших целых чисел

$$N > N_0.$$

Относительно числа N_0 («постоянная Виноградова») К. Г. Бороздкин в 1939 г. показал, что

$$N_0 \leqq e^{e^{e^{41,96}}}.$$

Н. Г. Чудаков в 1938 г. доказал, что «почти все» четные числа представляются как суммы двух нечетных простых чисел. Это означает: если $\nu(x)$ — число тех четных чисел $\leq x$, которые не представляются как суммы двух простых чисел, то $\lim\limits_{x \to \infty} \frac{\nu(x)}{x} = 0$.

Ю. В. Линник в 1946 г. дал иное доказательство теоремы Гольдбаха — Виноградова.

§ 83. В начале § 80 мы упоминали о трансцендентных числах, о том, что их существование было доказано Лиувиллем в 1844 г. Другое доказательство существования трансцендентных чисел дал Георг Кантор (в 70-х годах XIX в.), доказав, что множество всех алгебраических чисел — счетное, тогда как множество всех вещественных чисел даже в данном конечном интервале (хотя бы от 0 до 1) несчетное. Отсюда следует не только существование трансцендентных чисел, но и тот факт, что их множество несчетное, т. е. их, так сказать, гораздо «больше», чем алгебраических чисел.

В 1873 г. Эрмит доказал, что e (основание натуральных логарифмов) — число трансцендентное. В 1882 г. Линдеман доказал трансцендентность числа π. Русский математик Андрей Андреевич Марков в 1883 г. упростил эти доказательства.

После этого в течение свыше 40 лет почти никаких результатов в области теории трансцендентных чисел не было получено. В 1900 г. на Всемирном конгрессе математиков Д. Гильберт поставил 23 математических проблемы, решение которых требовало разработки новых методов. Седьмая из этих проблем Гильберта следующая: если $\alpha \neq 1$ — любое алгебраическое число, а β — любое алгебраическое иррациональное число, то будет ли α^β алгебраическим или трансцендентным числом? В частности, являются ли $2^{\sqrt{2}}$ и e^π — трансцендентными числами?

Упомянем еще статью **Д. Д. Мордухай-Болтовского** (1876—1952) «К теории трансцендентных чисел» (1919), где доказывается трансцендентность корня уравнения:

$$a_0 - a_1 x + a_2 \frac{x^2}{(2!)^{2!}} - a_3 \frac{x^3}{(3!)^{3!}} + \ldots \text{ in inf.} = 0,$$

где все $a_i > 0$ целые и $F < a_i < E$ (a_i ограничены сверху и снизу).

В 1929—30 гг. московский математик **Александр Осипович Гельфонд** (род. в 1906 г.) доказал, что если α — алгебраическое число, а $D > 0$ целое число, то $\alpha^{i\sqrt{D}}$ — трансцендентное число. В том же 1930 г. ленинградский математик **Родион Осиевич Кузьмин** (1891 — 1950) показал, что результат Гельфонда распространяется на случай вещественного показателя, т. е. при алгебраическом α и целом $D > 0$ число $\alpha^{\sqrt{D}}$ трансцендентное. Этим была доказана трансцендентность чисел $2^{\sqrt{2}}$ и e^π (ибо $e^\pi = (-1)^{-i}$) *).

В 1934 г. Гельфонд, углубив свой метод, дал доказательство трансцендентности чисел α^β, где α — алгебраическое число, отличное от 0 и 1, а β — алгебраическое иррациональное число; этим седьмая проблема Гильберта была полностью решена Гельфондом.

§ 84. Из других советских математиков, работавших в области теории чисел, назовем следующих:

Борис Николаевич Делоне (род. в 1890 г.) еще в 1922 г. дал полное решение уравнения $ax^3 + y^3 = 1$ (a — целое число), доказав, что кроме тривиального решения ($x = 0$, $y = 1$) оно может иметь не более одного решения в целых числах. Весьма большой не только теоретический, но и практический интерес имеют исследования Делоне по приложению теории тройничных квадратичных форм к кристаллографии, а также его исследования по геометрии чисел (ряд работ 30-х годов).

Николай Григорьевич Чеботарев (1894—1947), выдающийся советский алгебраист, имеет работы, относящиеся и к теории чисел. Он доказал существование бесконечного числа простых идеалов алгебраического поля, принадлежащих к данной подстановке. Это

---

*) Трансцендентность числа e^π доказал уже Гельфонд.

является обобщением известной теоремы Дирикле о бесчисленном множестве простых чисел в арифметической прогрессии (см. конец § 15).

Александр Яковлевич Хинчин (род. в 1894 г.) имеет ряд важных работ в так называемой метрической теории Диофантовых приближений.

Большим специалистом по теории чисел является также **Борис Алексеевич Венков** (род. в 1900 г.), имеющий важные исследования в теории тройничных форм и в арифметике кватернионов. Известна также его обзорная монография «Элементарная теория чисел» (1937 г.)

Желающим подробнее ознакомиться с достижениями советских математиков в области теории чисел можно рекомендовать книгу «Математика в СССР за тридцать лет» (1917—1947), раздел «Теория чисел».

УЧЕБНИКИ И ПОСОБИЯ ПО ТЕОРИИ ЧИСЕЛ.

И. В. Арнольд. Теория чисел. Пособие для пединститутов. Учпедгиз, 1939.

И. Г. Башмакова. Обоснование теории делимости в трудах Е. И. Золотарева. «Историко-математические исследования», вып. II, стр. 233—351.

В. П. Вельмин. Введение в теорию алгебраических чисел. Варшава, 1913.

Б. А. Венков. Элементарная теория чисел. ГТТИ, 1937.

И. М. Виноградов. Основы теории чисел. 6-ое изд. 1953.

И. М. Виноградов. Новый метод в аналитической теории чисел. Изд. Академии наук СССР, 1937.

Э. Гекке. Лекции по теории алгебраических чисел. ГТТИ, 1940.

А. О. Гельфонд. Трансцендентные и алгебраические числа. ГТТИ, 1952.

Д. А. Граве. Элементарный курс теории чисел. Киев, 1913.

Д. А. Граве. Арифметическая теория алгебраических величин. Том I. Квадратичная область. 1909—10 г. Киев, 1910 (литогр.)

Б. Н. Делоне. Петербургская школа теории чисел. Изд. Академии наук СССР, 1947.

Л. Е. Диксон. Введение в теорию чисел. Вып. 1. Изд. Академии наук Грузинской ССР, 1941.

П. Г. Лежен-Дирикле. Лекции по теории чисел в обработке и с добавлениями Р. Дедекинда. Перев. с немецкого под ред. Б. И. Сегала с приложением статьи Б. Н. Делоне «Геометрия бинарных квадратичных форм». ОНТИ, 1936.

Г. И. Дринфельд. Трансцендентность чисел π и e. Изд. Харьковского гос. университета, 1952.

Д. Ф. Егоров. Элементы теории чисел. ГИЗ, 1923.

И. И. Иванов. Теория чисел. Литогр. изд. СПб., 1910.

А. Е. Ингам. Распределение простых чисел. Перев. с англ. Райкова. ОНТИ, 1936.

Ю. В. Сохоцкий. Высшая алгебра. Часть вторая. Начала теории чисел. СПб., 1888.

А. Я. Хинчин. Великая теорема Ферма. Изд. 2-е. ГТТИ, 1932.

А. Я. Хинчин. Три жемчужины теории чисел. Гостехизд., 1947.

П. Л. Чебышев. Теория сравнений. Изд. III. СПб., 1901.

Н. Г. Чудаков. Введение в теорию L-функций Дирихле, Гостехизд., 1947.

ТАБЛИЦЫ ПЕРВООБРАЗНЫХ КОРНЕЙ И ИНДЕКСОВ

Простое число 5.

Первообразные корни: 2, 3.
Основание 2.

I.

N.	1	2	3	4
I.	4	1	3	2

N.

I.	1	2	3	4
N.	2	4	3	1

Простое число 7.

Первообразные корни: 3, 5.
Основание 3.

I.

N.	1	2	3	4	5	6
I.	6	2	1	4	5	3

N.

I.	1	2	3	4	5	6
N.	3	2	6	4	5	1

Простое число 11.

Первообразные корни: 2, 6, 7, 8.
Основание 2.

I.

N.	1	2	3	4	5	6	7	8	9	10
I.	10	1	8	2	4	9	7	3	6	5

N.

I.	1	2	3	4	5	6	7	8	9	10
N.	2	4	8	5	10	9	7	3	6	1

Простое число 13.

Первообразные корни: 2, 6, 7, 11.
Основание 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		12	5	8	10	9	1	7	3	4
1	2	11	6							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		6	10	8	9	2	12	7	3	5
1	4	11	1							

Простое число 17.

Первообразные корни: 3, 5, 6, 7, 10, 11, 12, 14.
Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		16	10	11	4	7	5	9	14	6
1	1	13	15	12	3	2	8			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	15	14	4	6	9	5	16	7
1	2	3	13	11	8	12	1			

Простое число 19.

Первообразные корни: 2, 3, 10, 13, 14, 15.
Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		18	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	5	12	6	3	11	15	17	18
1	9	14	7	13	16	8	4	2	1	

Простое число 23.

Первообразные корни: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.
Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		22	8	20	16	15	6	21	2	18
1	1	3	14	12	7	13	10	17	4	5
2	9	19	11							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	8	11	18	19	6	14	2	20
1	16	22	13	15	12	5	4	17	9	21
2	3	7	1							

Простое число 29.

Первообразные корни: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.
Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		28	11	27	22	18	10	20	5	26
1	1	23	21	2	3	17	16	7	9	15
2	12	19	6	24	4	8	13	25	14	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	13	14	24	8	22	17	25	18
1	6	2	20	26	28	19	16	15	5	21
2	7	12	4	11	23	27	9	3	1	

Простое число 31.

Первообразные корни: 3, 11, 12, 13, 17, 21, 22, 24.
Основание 17.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		30	12	13	24	20	25	4	6	26
1	2	29	7	23	16	3	18	1	8	22
2	14	17	11	21	19	10	5	9	28	27
3	15									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		17	10	15	7	26	8	12	18	27
1	25	22	2	3	20	30	14	21	16	24
2	5	23	19	13	4	6	9	29	28	11
3	1									

Простое число 37.

Первообразные корни: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35.
Основание 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		36	11	34	22	1	9	28	33	32
1	12	6	20	13	3	35	8	5	7	25
2	23	26	17	21	31	2	24	30	14	15
3	10	27	19	4	16	29	18			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		5	25	14	33	17	11	18	16	6
1	30	2	10	13	28	29	34	22	36	32
2	12	23	4	20	26	19	21	31	7	35
3	27	24	9	8	3	15	1			

Простое число 41.

Первообразные корни: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.
Основание 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7
4	1									

Простое число 43.

Первообразные корни: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.
Основание 28.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		42	39	17	36	5	14	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	15
4	38	18	21							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30
2	23	42	15	33	21	29	38	32	36	19
3	16	18	31	8	9	37	4	26	40	2
4	13	20	1							

Простое число 47.

Первообразные корни: 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45.
Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		46	30	18	14	17	2	38	44	36
1	1	27	32	3	22	35	28	42	20	29
2	31	10	11	39	16	34	33	8	6	43
3	19	5	12	45	26	9	4	24	13	21
4	15	25	40	37	41	7	23			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	6	13	36	31	28	45	27	35
1	21	22	32	38	4	40	24	5	3	30
2	18	39	14	46	37	41	34	11	16	19
3	2	20	12	26	25	15	9	43	7	23
4	42	44	17	29	8	33	1			

Простое число 53.

Первообразные корни: 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51.

Основание 26.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		52	25	9	50	31	34	38	23	18
1	4	46	7	28	11	40	48	42	43	41
2	29	47	19	39	32	10	1	27	36	6
3	13	45	21	3	15	17	16	22	14	37
4	2	33	20	30	44	49	12	8	5	24
5	35	51	26							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		26	40	33	10	48	29	12	47	3
1	25	14	46	30	38	34	36	35	9	22
2	42	32	37	8	49	2	52	27	13	20
3	43	5	24	41	6	50	28	39	7	23
4	15	19	17	18	44	31	11	21	16	45
5	4	51	1							

Простое число 59.

Первообразные корни: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56.

Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		58	25	32	50	34	57	44	17	6
1	1	45	24	23	11	8	42	14	31	22
2	26	18	12	27	49	10	48	38	36	4
3	33	7	9	19	39	20	56	41	47	55
4	51	2	43	13	37	40	52	53	16	30
5	35	46	15	28	5	21	3	54	29	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	41	56	29	54	9	21	15	32
1	25	14	22	43	17	52	48	8	21	33
2	35	55	19	13	12	2	20	23	53	58
3	49	18	3	30	5	50	28	44	27	34
4	45	37	16	42	7	11	51	38	26	24
5	4	40	46	47	57	39	36	6	1	

Простое число 61.

Первообразные корни: 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59.

Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		60	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	6	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	46
5	15	31	54	51	53	59	44	4	12	17
6	30									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44
2	13	8	19	7	9	29	46	33	25	6
3	60	51	22	37	4	40	34	35	45	23
4	47	43	3	30	56	11	49	2	20	17
5	48	53	42	54	52	32	15	28	36	55
6	1									

Простое число 67.

Первообразные корни: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63.

Основание 12.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		66	29	9	58	39	38	7	21	18
1	2	61	1	23	36	48	50	8	47	26
2	31	16	24	20	30	12	52	27	65	22
3	11	43	13	4	37	46	10	44	55	32
4	60	19	45	63	53	57	49	64	59	14
5	41	17	15	3	56	34	28	35	51	54
6	40	5	6	25	42	62	33			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		12	10	53	33	61	62	7	17	3
1	36	30	25	32	49	52	21	51	9	41
2	23	8	29	13	22	63	19	27	56	2
3	24	20	39	66	55	57	14	34	6	5
4	60	50	64	31	37	42	35	18	15	46
5	16	58	26	44	59	38	54	45	4	48
6	40	11	65	43	47	28	1			

Простое число 71.

Первообразные корни: 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69.

Основание 62.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		70	58	18	46	14	6	33	34	36
1	2	43	64	27	21	32	22	7	24	38
2	60	51	31	5	52	28	15	54	9	4
3	20	13	10	61	65	47	12	30	26	45
4	48	55	39	44	19	50	63	17	40	66
5	16	25	3	59	42	57	67	56	62	29
6	8	37	1	69	68	41	49	11	53	23
7	35									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		62	10	52	29	23	6	17	60	28
1	32	67	36	31	5	26	50	47	3	44
2	30	14	16	69	18	51	38	13	25	59
3	37	22	15	7	8	70	9	61	19	42
4	48	65	54	11	43	39	4	35	40	66
5	45	21	24	68	27	41	57	55	2	53
6	20	33	58	46	12	34	49	56	64	63
7	1									

Простое число 73.

Первообразные корни: 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68.

Основание 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		72	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44	1							

Простое число 79.

Первообразные корни: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77.

Основание 29.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		78	50	71	22	34	43	19	72	64
1	6	70	15	74	69	27	44	9	36	10
2	56	12	42	52	65	68	46	57	41	1
3	77	76	16	63	59	53	8	23	60	67
4	28	21	62	47	14	20	24	55	37	38
5	40	2	18	7	29	26	13	3	51	17
6	49	75	48	5	66	30	35	54	31	45
7	25	33	58	4	73	61	32	11	39	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		29	51	57	73	63	10	53	36	17
1	19	77	21	56	44	12	32	59	52	7
2	45	41	4	37	46	70	55	15	40	54
3	65	68	76	71	5	66	18	48	49	78
4	50	28	22	6	16	69	26	43	62	60
5	2	58	23	35	67	47	20	27	72	34
6	38	75	42	33	9	24	64	39	25	14
7	11	3	8	74	13	61	31	30	1	

Простое число 83.

Первообразные корни: 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80.

Основание 50.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		82	3	52	6	81	55	24	9	22
1	2	72	58	67	27	51	12	4	25	59
2	5	76	75	16	61	80	70	74	30	36
3	54	32	15	42	7	23	28	60	62	37
4	8	38	79	49	78	21	19	69	64	48
5	1	56	73	13	77	71	33	29	39	20
6	57	34	35	46	18	66	45	53	10	68
7	26	17	31	43	63	50	65	14	40	47
8	11	44	41							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		50	10	2	17	20	4	34	40	8
1	68	80	16	53	77	32	23	71	64	46
2	59	45	9	35	7	18	70	14	36	57
3	28	72	31	56	61	62	29	39	41	58
4	78	82	33	73	81	66	63	79	49	43
5	75	15	3	67	30	6	51	60	12	19
6	37	24	38	74	48	76	65	13	69	47
7	26	55	11	52	27	22	21	54	44	42
8	25	5	1							

Простое число 89.

Первообразные корни: 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86.

Основание 30.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		88	72	87	56	18	71	7	40	86
1	2	4	55	65	79	17	24	82	70	53
2	74	6	76	31	39	36	49	85	63	29
3	1	57	8	3	66	25	54	77	37	64
4	58	67	78	59	60	16	15	34	23	14
5	20	81	33	10	69	22	47	52	13	45
6	73	19	41	5	80	83	75	32	50	30
7	9	26	38	68	61	35	21	11	48	46
8	42	84	51	27	62	12	43	28	44	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		30	10	33	11	63	21	7	32	70
1	53	77	85	58	49	46	45	15	5	61
2	50	76	55	48	16	35	71	83	87	29
3	69	23	67	52	47	75	25	38	72	24
4	8	62	80	86	88	59	79	56	78	26
5	68	82	57	19	36	12	4	31	40	43
6	44	74	84	28	39	13	34	41	73	54
7	18	6	2	60	20	66	22	37	42	14
8	64	51	17	65	81	27	9	3	1	

Простое число 97.

Первообразные корни: 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92.

Основание 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		96	86	2	76	11	88	53	66	4
1	1	82	78	83	43	13	56	19	90	27
2	87	55	72	79	68	22	73	6	33	47
3	3	26	46	84	9	64	80	41	17	85
4	77	71	45	44	62	15	69	60	58	10
5	12	21	63	14	92	93	23	29	37	65
6	89	32	16	57	36	94	74	51	95	81
7	54	25	70	20	31	24	7	39	75	42
8	67	8	61	91	35	30	34	49	52	18
9	5	40	59	28	50	38	48			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	3	30	9	90	27	76	81	34
1	49	5	50	15	53	45	62	38	89	17
2	73	51	25	56	75	71	31	19	93	57
3	85	74	61	28	86	84	64	58	95	77
4	91	37	79	14	43	42	32	29	96	87
5	94	67	88	7	70	21	16	63	48	92
6	47	82	44	52	35	59	8	80	24	46
7	72	41	22	26	66	78	4	40	12	23
8	36	69	11	13	33	39	2	20	6	60
9	18	83	54	55	65	68	1			

ОГЛАВЛЕНИЕ

Глава IV. Квадратичные вычеты

Стр.

Глава V. Первообразные корни и индексы

Глава VI. Некоторые сведения о квадратичных формах

Глава VII. Работы по теории чисел русских и советских математиков

Техредактор *Г. П. Стецюк* Корректор *К. Летуновская*

Подписано к набору 19/II 1954 г. Подписано к печати 7/VI 54 г. БЦ 12840. Тираж 10 000.
Бумага 60 × 92[1]/16. Бум. л. 6,38. Печ. л. 12[3] . Учет.-изд. л. 14. В 1 печ. л. 43 000 зн. Зак. 476.
Цена 4 руб. 20 коп.

Отпечатано с матриц книжной ф-ки им. Фрунзе Главиздата Министерства культуры УССР
в 4-й тип. Углетехиздата. Харьков, ул. Энгельса, 11. Зак. 2065.

ЗАМЕЧЕННЫЕ ОПЕЧАТКИ

Страница	Строка	Напечатано	Должно быть
19	13 снизу	$a_0[(a+zp)^m - a_m]$	$a_0[(a+zp)^m - a^m]$
37	6 сверху	r_{m+1}	r_{n+1}
61	14 „	сравнение	сравнения
87	15 „	$(y-1)!$	$(p-1)!$
131	13 снизу	2, 5, $20k+3$,	2, 5, $20k+1$, $20k+3$,
132	3 „	12, —13.	12, —13, 19, 44.
153	15 и 16 сверху	г) $+9$; д) $+6$; $+17$; ± 26; $+44$.	г) ± 9; д) ± 6; ± 17; ± 26; ± 44.
153	6 снизу	б) $+23$.	б) ± 23.
159	15 сверху	$xy_2 + x_2y_1$	$x_1y_2 + x_2y_1$
162	14 „	$2q$ не делится на 4.	$2p$ не делится на 4.

А. К. Сушкевич. „Теория чисел“.